Aalto University
School of Science
Master's Programme in Computer, Communication and Information Sciences

Hannu Seppänen

Modelling IoT Business Opportunities

Master's Thesis
Espoo, October 7, 2018

Supervisor: Professor Martti Mäntylä, Aalto University
Advisors: Jussi-Pekka Erkkola MA
Kai Puustinen M.Soc.Sc.

Aalto University
School of Science
Master's Programme in Computer, Communication and Information Sciences

ABSTRACT OF MASTER'S THESIS

Author:	Hannu Seppänen		
Title:	Modelling IoT Business Opportunities		
Date:	October 7, 2018	**Pages:**	111
Major:	Software and Service Engineering	**Code:**	SCI3043
Supervisor:	Professor Martti Mäntylä		
Advisors:	Jussi-Pekka Erkkola MA Kai Puustinen M.Soc.Sc.		

Our world is becoming increasingly digitized. Digitalization has changed and is changing business models at accelerating pace and creating new revenue and value-producing opportunities. We are now witnessing the age where the digital technologies are harnessed for our advantage - as the physical technologies were harnessed in the first industrial revolution. Still, the digital world and the physical world are separated from each other. This is the one significant issue, that the Internet of Things (IoT) is about to change. The vision of the IoT is to connect people and devices and produce a vast variety of new goods and services.

As the IoT is a novel phenomenon, it can be a difficult concept to define. It can be difficult to create a comprehensive understanding on what the IoT is and what kind opportunities it has to offer. In addition, The IoT is a complex phenomenon in terms of monetization. It can be difficult to create a comprehensive understanding on where the real value of the IoT comes from.

The goal of this study is to to create a framework of possible IoT business opportunities for the target company. This is done by creating a conceptualization that unfolds the different roles there are in IoT business for the target company to take or aim for. In addition to the conceptualization, there is also a need to create better understanding of the customership and value proposition related to the IoT business, and recognize the most important barriers of adoption and capabilities required for managing the barriers of adoption.

Keywords:	Internet of things, IoT, conceptualization, framework, business models
Language:	English

Aalto-yliopisto
Perustieteiden korkeakoulu
Master's Programme in Computer, Communication and Information Sciences

DIPLOMITYÖN TIIVISTELMÄ

Tekijä:	Hannu Seppänen		
Työn nimi:	IoT-liiketoiminnan mallintaminen		
Päiväys:	7. Lokakuuta 2018	**Sivumäärä:**	111
Pääaine:	Software and Service Engineering	**Koodi:**	SCI3043
Valvoja:	Professori Martti Mäntylä		
Ohjaajat:	MA Jussi-Pekka Erkkola VTM Kai Puustinen		

Digitalisaatio on muuttanut ja muuttaa liiketoimintamalleja kiihtyvällä vauhdilla luoden uusia mahdollisuuksia arvontuotolle. Todistamme nyt aikakautta, jossa digitaaliset teknologiat valjastetaan käyttöön kuten fyysiset teknologiat valjastettiin ensimmäisessä teollisessa vallankumouksessa. Siltikin digitaalinen ja fyysinen maailma ovat olleet tähän asti erossa toisistaan. Tämä on merkittävin asia, jonka esineiden internet tulee muuttamaan. Esineiden internetin visiona on yhdistää ihmiset ja laitteet ja luoda laaja valikoima uusia tavaroita ja palveluita.

Koska esineiden internet on uusi ilmiö, sen määritteleminen voi olla vaikeaa. On haastavaa luoda kattavaa käsitystä siitä, mitä esineiden internet on ja millaisia mahdollisuuksia se tarjoaa. Lisäksi esineiden internet on minimutkainen ilmiö kaupallistamisen kannalta. On haastavaa luoda kattavaa käsitystä mistä esineiden internetin todellinen arvo tulee.

Tämän opinnäytteen tavoitteena on luoda viitekehys, jonka avulla kohdeyritys voi paremmin hahmottaa esineiden internetin tarjoamia liiketoimintamahdollisuuksia. Tämä mahdollistetaan hahmottamalla erilaiset roolit, joihin kohdeyritys voi asettua. Viitekehyksen lisäksi opinnäytteen tavoitteena on luoda parempi ymmärrys IoT-liiketoimintaan liittyvistä asiakkuuksista ja arvolupauksista, sekä tunnistaa tärkeimmät käyttöönoton esteet sekä tarvittavat kyvykkyydet niiden hallitsemiseksi.

Asiasanat:	Esineiden Internet, IoT, kehys, liiketoimintamallit
Kieli:	Englanti

Contents

Chapter 1

Introduction

This chapter introduces the topic of the thesis and the motivation for the study. This chapter first describes the research problem and the scope of the study. After that, the research questions are presented and the research design and process defined. The chapter ends with a brief overview of the structure of the study.

1.1 Research problem and scope

As the Internet of Things (IoT) is a novel phenomenon, it can be a difficult concept to define. It can be difficult to create a comprehensive understanding on what the IoT is and what kind opportunities it has to offer. Currently, It is not possible for the target company to create a sufficiently comprehensive understanding of the opportunities offered by the IoT. In addition, The IoT is a complex phenomenon in terms of monetization. It can be difficult to create a comprehensive understanding on where the real value of the IoT comes from. Therefore, it is interesting for the target company to understand what kind of business possibilities the IoT can offer.

Based on the aforementioned research problems, the first research question is formed as follows:

Q1: What aspects should the target company consider when starting IoT business?

The second research question is formed as follows:

Q2: What kind of barriers of adoption are associated to the starting of IoT business and what kind of capabilities are required for managing them?

As a result of the research problems, the goal of this study is to create a view or a framework of possible IoT business opportunities for the target company. This is done by creating a conceptualization that aims to unfold the different roles there are in IoT business for the target company to take or aim for. In addition, this study aims to provide a understanding of the customership and value proposition related to the IoT business, and recognize the most important barriers of adoption and capabilities required for managing the barriers of adoption.

1.2 Research methodology and process

This section describes the used research methods in this thesis. In addition, the design and the process of the study is described. Research can be categorized into two distinct types, qualitative and quantitative research. The qualitative research concentrates on words and observations for expressing reality and aims to describe people in natural situations. The quantitative research trusts in numbers that represents opinions or concepts. (Amaratunga et al, 2002). This study uses the qualitative research approach.

It can be somewhat difficult to find a definitive statement on what the qualitative research actually is. This is because the theory and methodology are usually quite closely interrelated in qualitative research. Qualitative research is conducted through and intense and sometimes prolonged contact with a real life situation. These situations are usually reflective of the everyday life of individuals, groups, societies, and organizations. One major feature of qualitative research is that it focuses on naturally occurring, ordinary events, in natural settings. Another feature of qualitative research is the richness and holism of data that has a strong potential for revealing complexity. (Amaratunga et al, 2002). These are the reasons that makes the qualitative research approach suitable for this study.

A case study approach was used in this study for understanding and testing the created conceptualization. It is reasonable to use case study approach whenever an empirical research must examine a contemporary phenomenon in its real-life context. This is especially true when the boundaries between the phenomenon and context are not clearly evident. Case study approach is relevant for studying knowledge utilization, because the topic covers a phenomenon that seems to be inseparable from its context. (Yin, 1981).

Once the research problem and the goals of the study had been identified, the study started as a desk study with a literature review. The desk study aimed

to clarify, what IoT and IoT business are, and to clarify, what are the key elements of IoT. In addition, the desk study aimed to identify the relevant existing phenomena around the problem scope in order to form the conceptualization of IoT business opportunities. This included reading academic research papers, company white papers, and relevant blogs and articles. In addition, discussions with the target company representatives were held and two internal workshops were organized for creating deeper understanding about the perspectives towards IoT from the target company's point of view. The empirical part of the study was conducted as a case study. One IoT related case was selected to be viewed through the created conceptualization. The overall process of the study is presented in figure 1.1.

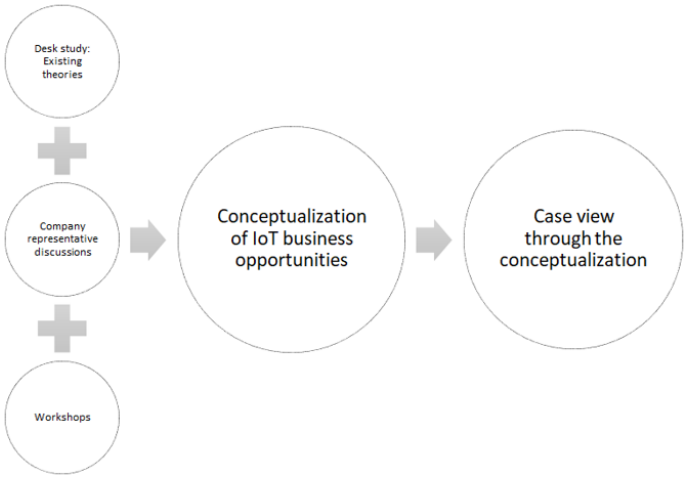

Figure 1.1: The design and process of the study.

1.3 Structure of the thesis

This section describes the structure of the study. The first chapter presents the context of the study, followed by the research problem and research questions and a overview of the design and process of the study. The second chapter presents the background for the study. The second chapter describes the definitions of the key concepts, gives an overview of the IoT and IoT business in general and also presents the target company. The third chapter describes the key phenomenon affecting IoT business and creates the conceptualization of IoT business opportunities. The third chapter also creates an overview of the capabilities required when considering starting IoT business, as well as describes the barriers of adoption affecting IoT. Chapter four describes one

actual IoT use case viewed through the created conceptualization. Finally, in chapter five, the research questions are answered and the study is concluded with suggestions for future work and research.

Chapter 2

Background

Our world is becoming increasingly digitized. Digitalization has changed and is changing business models at accelerating pace and creating new revenue and value-producing opportunities. We are now witnessing the age where the digital technologies are harnessed for our advantage - as the physical technologies were harnessed in the first industrial revolution. (Brynjolfsson and Mcafee, 2016).

Still, the digital world and the physical world are separated from each other. This is the one significant issue, that the IoT is about to change. The vision of the IoT is to connect people and devices and produce a vast variety of new goods and services. This new connection between digital world and physical objects is supposed to improve quality of life by, for example offering conveniently accessible health and fitness services, or by enhancing the management of homes, offices, worksites, factories or entire cities. (Buyya and Dastjerdi, 2016).

In this chapter, the key concepts and terms related to the IoT are first defined. Secondly, the meaning of the IoT is explained. Thirdly, an overview of the possibilities that the IoT can offer to users and businesses is presented. Finally, this chapter presents the target company, to whom the conceptualization of IoT business opportunities is created.

2.1 Definitions of key concepts

This chapter summarizes the key concepts used and discussed in this thesis.

Actuator

A mechanism that performs a physical task based on input from a connected system (Gates, 2017).

Artificial Intelligence (AI)

The theory and development of computer systems which are able to perform tasks normally requiring human intelligence. Such tasks can be for example, visual perception, speech recognition, decision-making, and translation between languages (Marr, 2018).

Big Data

A broad term for any collection of data sets so large and complex that it becomes difficult to process with traditional data processing applications (Press, 2014).

Cloud Computing

The use of various services, like software development platforms, servers, storage and software, over the internet (Techopedia, 2018).

Cyber-Physical Systems (CPS)

Transformative technologies for managing interconnected systems between its physical assets and computational capabilities (Lee, Bagheri and Kao, 2015).

Data Mining

Process of analyzing data and transforming it into insight that informs business decisions. Data mining software enables organizations to analyze data from different sources in order to detect patterns (Galletto, 2018).

Digitalization

Process of moving to digital business. Digitalization is the use of digital technologies to change a business model and provide new revenue and value-producing opportunities (Gartner, 2018).

Digitization

Digitization is the process of changing from analog to digital form (Gartner, 2018).

Ecosystem

The term ecosystem is used for describing a variety of concepts. The term is used for example to describe biological ecosystems, digital ecosystems, and business ecosystems. A biological ecosystem consists of an environment, and actors in it (Boley and Chang, 2007). Digital ecosystems can be defined as software systems that utilize the properties of biological ecosystems, like robustness, scalability and self-organization (Briscoe and De Wilde, 2006). A business ecosystem is a economic community that consists of interacting organizations and individuals (Moore, 1996).

Edge Computing

Concept of computing where the computing is done at, or near the source of the data, instead of relying on the cloud (Miller, 2018).

Fog Computing

A concept that extends the concept of cloud computing to the network edge, making it ideal for the IoT and other applications that require real-time interactions (Butler, 2018).

Industrial Internet

The integration of machine learning, big data technology, sensor data, and machine-to-machine communication automation, which is done with the knowledge that the IoT will be scaled and driven by enterprises. The main idea behind the Industrial Internet is that smart machines can more accurately capture and communicate data to help companies find problems sooner and increase overall efficiency (Gates, 2017).

Internet of Things (IoT)

A network of physical objects added with sensors and actuators, capable of capturing data from surrounding environment autonomously and capable of acting autonomously and intelligently based on the gathered data (Gates, 2017). The term Internet of Things is often used interchangeably with terms like Industrial Internet, Industrial Internet of Things, Web of Things, Internet of Everything and M2M - just to name a few. The concepts behind these terms are very similar, but usually the things and the environment in which they act differs (Wheatley, 2013).

Machine Learning

Science of getting computers to learn and act like humans do, and improve their learning over time in autonomous fashion by feeding them data and information in the form of observations and real-world interactions (Faggella, 2017).

Machine-to-Machine (M2M)

A network setup that allows connected devices to communicate freely between a large number of devices. M2M often refers to the use of distributed systems in industrial and manufacturing applications (Gates, 2017).

Platform

Platforms can be defined in several ways. In their core platforms are environments, either technical, like software systems or physical, like places or goods, connecting different actors that derive value from others that participate in the platform (Church, 2017; Van Alstyne, Parker and Choudary, 2016). These different actors consists of the platform owner, users, and complementary business partners, often called complementors, which all utilize and benefit from the platform's base functionality (Suarez and Kirtley, 2012). Platforms can also be seen from different theoretical perspectives: through economics, which sees platforms as multi-sided markets, or through engineering, which sees platforms as technological architectures (Gawer, 2104).

Sensor

A device or component that perceives and responds to physical input from the environment (Gates, 2017).

Sensor network

A group of sensors with a communications infrastructure intended to monitor and collect data from multiple locations (Gates, 2017).

Smart connected device

Physical components or devices incorporated with built-in sensors and actuators that collect data to help users or other devices make informed decisions and monitor or affect outside events (Gates, 2017).

Ubiquitous computing

A method of enhancing the use of computers by making several computers available throughout a physical environment, but making them effectively invisible to the user (Gates, 2017).

2.2 IoT explained

The history of mankind has seen three major industrial revolutions. The first industrial revolution came with the steam engine and the mechanization of work. The second industrial revolution came with electricity along with the assembly line and mass production. The third industrial revolution came with the birth of computers, enabling automation and robotisation. Now we are entering to the era of fourth industrial revolution; the era of smart connected products, ubiquitous computing, big data, artificial intelligence, machine learning, digitalization and cyber-physical systems. (Marr, 2016; Hermann, Pentek and Otto, 2016).

The origins of the IoT can be traced to the internet-connected coke machine of Carnegie Mellon University computer science department in the eighties, and the internet-connected coffee machine of Cambridge University in the nineties. Later in the nineties, studies of multiple researchers from different approaches helped to shape the vision of the IoT. (Chen, 2017). The term Internet of Things was presumably first used by Kevin Ashton in 1999. He used the term when he described the usage of RFIDs in supply-chain management. With the term he tried to describe that today, computers and the internet are practically completely dependent on human beings for information. Nearly all of the data available on the internet was first captured and created by humans. The problem is that - because of limited time, attention, and accuracy - humans aren't very good at capturing data about things in the real world. If we had computers capable of knowing everything about every physical object, using data gathered without help from humans, we would be able to track and count everything. This could then vastly reduce waste, loss, and costs. We would even be able to know when objects needed replacing, repairing, or recalling, or whether the objects were usable or past their lifecycle. (Ashton, 2009).

Since then, the term Internet of Things has evolved to a umbrella term that refers to anything connected to the internet. The anything can be a traditional computing device, like laptop, tablet, or a smartphone, or it can be basically any device which is made internet enabled, like home appliances, cars, wearables, and security cameras, just to name a few. (Christensson, 2015). In order for a device to be part of the Internet of Things, it needs to have certain characteristics. The characteristics are related to the things, data, communication, intelligence, action, ecosystem, and connectivity. Things refer to anything that can be individually identified and connected, ranging from sensors to appliances and even humans and animals. Data refers to

the ability to collect data from the connected devices. The collected data is the first step towards action and intelligence. Communication refers to the ability to communicate the collected data from the device. Intelligence comes as a result from the sensing capabilities in the devices and intelligence gathered from data analytics. Action is the consequence of the intelligence. Action can be manual, done by the user, or autonomous, done by the device. Ecosystem refers to the environment in which the IoT resides. Finally, connectivity refers to the capability to connect the devices or sensor to other devices, actuators, or processes through some network. (i-Scoop, 2018).

It is expected, that the IoT will have a major disruptive effect on individuals, society, and businesses. The connected devices, like household appliances, healthcare devices, and home security systems can greatly improve the quality of life for individuals. The optimization of resource usage can be greatly improved with help of the IoT. Individuals can control better the consumption of food, water, and power. Businesses can better optimize the usage of assets, like material usage, supply chains, and distribution channels. Public facilities, like hospitals, libraries, and police offices are able to offer better service with the help of the IoT. The overall efficiency can be improved when the physical devices are able to sense the environment, communicate with each other, and act autonomously based on the information collected. The IoT can also have a major impact on the market structure. For example, when individual consumer's behavior and preferences can be recorded with the devices, customized marketing strategies can be generated automatically. (Chen, 2017)

As the IoT will open numerous possibilities and opportunities for economy and individuals, it will also present many risks and challenges. These risks and challenges include data security challenges, privacy challenges, and challenges related to technology. Even without the countless devices connected to the internet, there are challenges to keep the data of users secure. The responsibilities of the privacy of users are very unclear at this point. The value of the IoT for businesses will mainly come from the data collected and analyzed from the devices which will cause challenges to the privacy of the users. The IoT today is technologically very immature. There is a lack of standardization and best practices, which can cause challenges in the future. (Chen, 2017)

2.3 IoT business explained

The common belief seems to be, that the IoT will have a great impact on the economy. The social and economical impact will most likely be gradual, and eventually significant. The IoT will carry the transformation into digital business, facilitate new business models, improve efficiency, and increase employee and customer engagement for majority of enterprises. The estimations on the economic impact of the IoT varies depending on sources, but it seems that the economic impact will be trillions in the next ten years (Manyika et al, 2015; Columbus, 2017). At the same time, the amount of IoT devices will be counted in billions. (Hung, 2017). Even though the amount of connected devices is measured in billions, it still means that more than 99 percent of the devices that could leverage IoT are not connected, so the potential for growth is massive (Cisco, 2013; IBM, 2018).

The entities, that are expected to see the benefits of IoT include consumers, businesses, and governments. The IoT is expected to have influence to every industrial sector in some way. Some of these industrial sectors include for example, manufacturing, transportation, defense, agriculture, infrastructure, retail, logistics, banks, connected homes, smart buildings, smart cities, healthcare, and many more. (Meola, 2018). The application possibilities of the IoT are practically limitless. We can already see many practical IoT applications in use in many domains like for example, predictive maintenance, asset tracking, consumption monitoring, health conditions monitoring and treatment, traffic coordination, connected fleet management, network management and outage detection, and self-driving cars, just to name few (Rodriguez and Stammati, 2018).

2.4 The target company

The target company to which the conceptualization of IoT business opportunities presented in this thesis is created, is one of the biggest retailers in northern Europe. It has operations in seven countries, Finland, Sweden, Norway, Estonia, Lithuania, Belarus, and Poland. The target company operates in three different trading sectors: grocery trade, building and technical trade, and car trade. The trading sectors where the target company operates are all sectors, where the IoT will most likely have a major disruptive impact. For that reason, there is a need to create understanding of the possible effects and possibilities that the IoT will cause.

The conceptualization of IoT business opportunities presented in this thesis is mainly targeted to the building and technical trade of the target company. The building and technical trade of the target company offers multichannel services for building, renovation, and building services engineering to both, consumer customers as well as business customers. The conceptualization of IoT business opportunities presented in this thesis doesn't make difference between consumer customers and business customers, but aims to be usable for both. Even though the conceptualization is targeted to the building and technical trade and the one case, where the conceptualization is used for understanding the IoT business possibilities is from building and technical trade, it can still be used in other sectors as well.

Chapter 3

Modelling IoT business opportunities

Understanding the commercial potential of the IoT from the point of view of the target company is one of the main targets of this thesis. For achieving this, a conceptualization of the IoT business opportunities is created through a framework which combines the possible roles and positions for the target company to take.

The main objective of this chapter is to create a framework of possible roles and positions for the target company to take. The objective is expressly to describe the framework from the point of view of the target company. Before the framework can be described, it is important to understand the overall architecture and the technology stack of the IoT, the expanding of industry boundaries caused by the IoT, and also to create a comprehensive overview of IoT business models.

3.1 The structure of the IoT

A generally accepted, 3-layered high level architecture (see fig. 3.1) of the IoT consists of perception layer, network layer, and application layer. The perception layer handles the identification of the objects and information gathering. The network layer handles the information transmission and processing. (Wu et al, 2010). The application layer acts as a front end of the whole IoT architecture through which the IoT will be exploited (Abdmeziem, Tandjaoui and Romdhani, 2016).

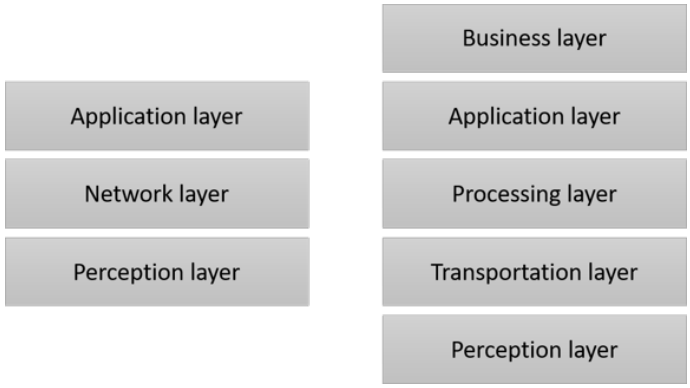

Figure 3.1: 3-layer and 5-layer IoT architecture. (Wu et al, 2010).

Wu et al (2010) present a more comprehensive 5-layered architecture of the IoT (see fig. 3.1), which consists of perception layer, transportation layer, processing layer, application layer, and business layer. The perception layer and the transportation layer act same as in the 3-layered architecture, handling the perception of physical properties of the objects via sensors and transmission of the data from the perception layer to the processing layer. The processing layer handles the storing, analysing and processing of the data received from the transportation layer. The application layer acts same as in the 3-layered architecture, acting as the front end of the IoT. The business layer handles the managing of the IoT, including the business models and profit models. (Wu et al, 2010).

The IoT products create a completely new requirements for technology infrastructure for companies to build and support. The IoT technology stack (see fig. 3.2) consists of multiple layers, including product hardware and embedded software, connectivity, and a product cloud, which consists of a application platform and software applications running on remote servers. The IoT technology stack also includes a suite of security tools, a gateway for external information sources and integration capabilities with enterprise information systems. (Porter and Heppelmann, 2014:70).

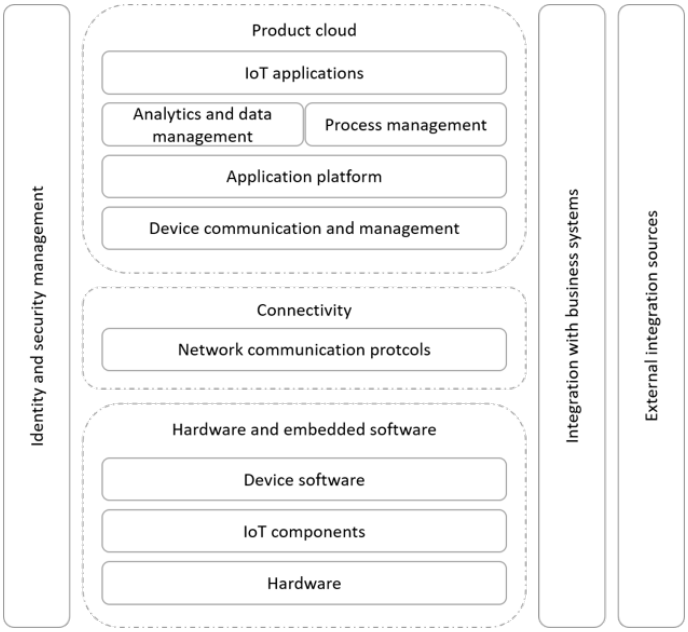

Figure 3.2: The IoT technology stack (Porter and Heppelmann, 2014).

The general IoT technology stack consists of three core layers: hardware and embedded software, connectivity, and product cloud. The hardware and embedded software layer consists of physical hardware of the device, IoT components, like sensors, actuators, processors, and connectivity components. The connectivity layer consists of network protocols that enable the communication between the device and the cloud. The product cloud layer consists of the software components that handle the communication, provision, and management of the devices, application platform, software components that handle the storing, processing, and analyzing of the sensor data, software components that are responsible for the definition, execution, and monitoring of processes, and the IoT applications, that handle the interactions between the users and the IoT devices. The IoT technology stack also includes a suite of security tools, that are responsible for user authentication and access management, as well as the security across the different layers. In addition, the IoT technology stack also includes a gateway for external information sources and integration capabilities with enterprise information systems for additional data. (Porter and Heppelmann, 2014).

The IoT devices present a completely new set of functionality and capabilities. Porter and Heppelmann (2014:70-72) group these capabilities into four areas: monitoring, control, optimization and autonomy (see fig. 3.3). Each capability can have value on its own and each capability can act as a enabler

for another capability. It is also possible for a IoT product to incorporate all four capabilities.

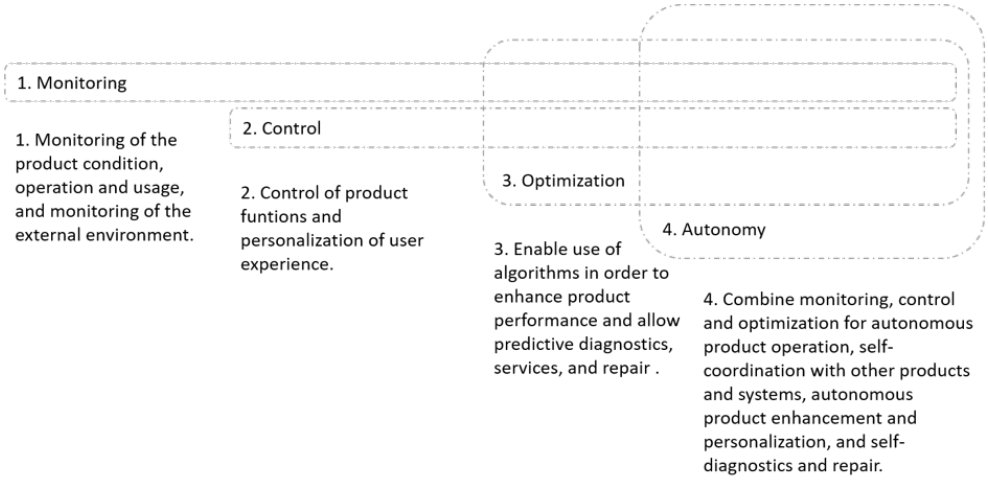

Figure 3.3: Capabilities of IoT products (Porter and Heppelmann, 2014).

The IoT products enable comprehensive monitoring of different attributes of the device, like condition, operation, and monitoring of surrounding environment through sensors and external data sources. The IoT products can be controlled with remote commands or via algorithms built into the device or residing in a cloud. The vast amounts of monitoring data created by the IoT product combined with the capability to control the products creates the possibility for optimization for companies. With IoT products companies can optimize product performance in many ways, like for example by enabling predictive diagnostics or by enabling predictive service and repair. The first three capabilities, monitoring, control and optimization combined create a possibility for autonomy, which has been virtually unattainable before now. (Porter and Heppelmann, 2014:70-72).

The increasing capabilities of the IoT products not only affect the competition between companies within industries, but expand the industry boundaries (see fig. 3.4). For the companies to able to answer the broader need of the customer, they need to widen the competitive boundaries of an industry with a set of related products. This shifts the competition from a discrete product to a broader product system, where the company is just one actor. This, however, is not enough but the industry boundaries are expanding even beyond product systems towards systems of systems. Systems of systems are a set of disparate product systems coupled with external information that can be coordinated and optimized. (Porter and Heppelmann, 2014:75-77).

Figure 3.4: Redefining industry boundaries (Porter and Heppelman, 2014).

Figure 3.4 shows the evolution of a product which leads to expansion of industry boundaries. In this example a vehicle is first equipped with sensors and actuators and connectivity creating a smart, connected product. When this smart, connected product is then integrated to, for example farm equipment system, a product system is created. The product system usually consists of more than one actor. When the product system is integrated to, for example weather data system and irrigation system, a system of systems is created.

The IoT architecture is linked to the creation of IoT business models. A key feature of the IoT business models is that the modular layered architecture of the IoT can be separated from one another. In this way the IoT objects can represent a combination of elements across these different layers. The separation of devices, content and information infrastructures enables multiple stakeholders to contribute across the layers. In this way, the layers can be seen as sources of value creation and they lay the foundation for different business models. (Turber et al, 2014). The next chapter describes the business model archetype, business model innovation process, value and revenue generation in the IoT-domain, and introduces some business model patterns for IoT-enabled products.

3.2 IoT business models

For understanding the business models and commercial potential of the IoT from the point of view of the target company, it is first important to understand what does a business model generally mean. The operating conditions of businesses today are mainly determined by technological progress, service orientation, digitalization, and the increasing significance of cooperation and ecosystems of different companies, which expands the boundaries of individual companies and industries. A business model acts as a unit of analysis by offering a logical and consistent approach to the design and execution of the business (Bucherer and Uckelmann, 2011:255). The term business model has been a part of the managerial literature since the end of the 1990s. A business model can be described as a unit of analysis to describe how the

business works in a company (Gassmann, Frankenberger and Csik, 2013:1). More specifically, a business models describes the rationale of how a company creates, delivers and captures value (Osterwalder and Pigneur, 2010).

Gassmann, Frankenberger and Csik (2013:2) describe a conceptualization of a business model which consists of four dimensions (see fig. 3.5), the who, the what, the how, and the value. The four dimensional conceptual model is at the same time, simple enough to understand and use, and comprehensive enough to provide a clear overall picture of the business model architecture.

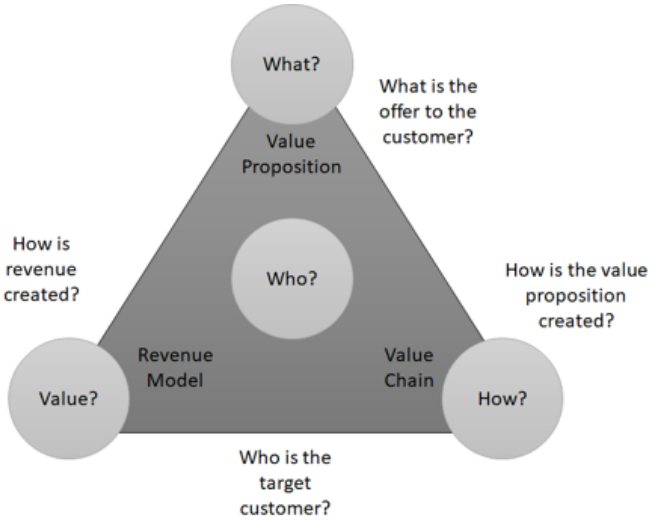

Figure 3.5: Business model definition. (Gassmann, Frankenberger and Csik, 2013).

Every business model is connected to and serves a certain customer group. Thereby, the who dimension defines who is the customer. In every business model the offer to the customer, or what the customer values, needs to be described. Thus, the what dimension defines the customer value proposition. For the company to be able to build and distribute the value proposition, the company has to manage numerous processes and activities. Thereby, the how dimension defines the processes, activities, resources, capabilities and their orchestration. Finally, business model also needs to be financially viable. Thus, the value dimension defines revenue model and answers the question of how the business model can be monetized (Gassmann, Frankenberger and Csik, 2013:2).

Generally, it can be said that technology in itself has no objective value. The economic value of technology will only appear when it is commercialized through a business model. The same technology commercialized through two different business models will result two different outcomes (Chesbrough, 2010:354-355). Nowadays, for the companies to stay competitive in a rapidly changing business environment, it has become even more critical to adapt and innovate in every dimension. Just focusing on product and process improvements can be insufficient. The changing business conditions require companies to look and possibly change their whole way of doing business. (Bucherer and Uckelmann, 2011:257-258).

Business model innovation is a process, that results in a qualitatively new business model that differs distinctly from the previous business model. Business model innovation is usually triggered in companies when external factors, such as technology innovations, increased competition, market changes, or legal or regulatory changes happen. Business model innovation is used in companies for gaining competitive advantage or for differentiating from competitors. Different approaches for business model innovation, like for example opportunity-driven approach and forward-looking approach can be used. In opportunity-driven approach companies can benefit from first-mover advantage. However, when an existing business model starts to decline, it can already be too late to change direction. In the forward-looking approach business model innovation is used more proactively for market share capture and new market entry. (Bucherer and Uckelmann, 2011:258). Some of the most successful companies today have changed their business models radically because of changes in external factors (see table 3.1). The success of these companies builds on technological innovation and services, which replaced some traditional businesses.

Company	Traditional business	Initial business model innovation	Further development
Amazon	Book trade	Online shopping Automated distribution model Collaborative filtering	Shopping portal Digitalisation (mp3, books) Terminals (Kindle) Mobile payments Amazon web services (incl.billing) Collaborative filtering
eBay	Classifieds Flea markets Auctions	Online auctions	Shopping portal payment services (PayPal)
Google	Yellow pages	Hypertext web search Prioritised advertisements	Terminals (Android) Video (You Tube) Maps (Google Maps) Web based software (e.g. Google Docs) Digitalised books Payment services (Checkout)

Table 3.1: Traditional business vs. business model innovation (Bucherer and Uckelmann, 2011).

The Internet acts as a main enabler for success in the examples above. Fast and agile logistic services provide advantage over traditional concepts. Well accepted billing systems create competitive advantage. Move towards mobility that allows ubiquitous access to digital content is another key to success. It can be expected that the new business models that are based on the IoT will change and replace some traditional business models in a same way. (Bucherer and Uckelmann, 2011:259-260). There are predictions that the disruption caused by IoT will bypass the disruption caused by the Internet (Burrus, 2014; Silverstein, 2017).

A typical business transaction today can be defined by a physical product or a service, and by information and money streams. It is good to notice, that unlike in a service-oriented business, like for example services related to the Internet, in IoT there is always a link to the physical product. Because of the higher level of visibility and control mechanisms in the IoT, it can be seen as an approach, that will align the different value streams. In addition, in the IoT, the data and the information processed from it may prove to be a major source of value creation and thus form to be the value proposition. (Bucherer and Uckelmann, 2011:260).

Traditionally, the money stream has been solely dependent on the product stream. The customers expect the information to be included free of charge.

Usually there is no separate price for information defined, but instead the costs of the information are hidden in the product price. However, it seems that the willingness to pay for information is slowly increasing. The IoT makes more and especially more detailed information available for the user, which makes new value proposition scenarios, like provision of additional product-related data or exact billing based on actual use possible. (Bucherer and Uckelmann, 2011:260).

New value propositions requires also rethinking the financial aspects. Historically, the value discussions in the IoT have revolved around cost. The costs of creating an IoT device can be calculated rather well, but finding a return on investment instead is more difficult. Therefore, the revenue generation should be considered as an important aspect when designing IoT devices or services. The pricing of information can for example compensate for the provided infrastructure and information generation. Usage based pricing or subscription fees can be used, and information brokers may be introduced to the framework. In the selling of physical products, the value chain usually ends with the delivery of the product to the customer, but in the exchange of information it spans to a much longer time and may include multiple different actors. Figure 3.6 depicts the information exchange and actors involved in the IoT environment. (Bucherer and Uckelmann, 2011:263-265).

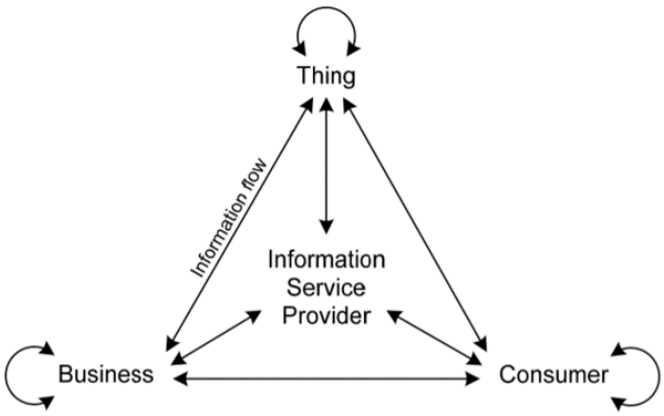

Figure 3.6: IoT information flows and information providers (Bucherer and Uckelmann, 2011).

The actors include the things, consumers, businesses, and service providers. The things can be for example products, that communicate their identity and status through sensors or data processing units or actuators. Businesses and

consumers can provide additional information, like for example information from other systems, like ERP systems, or manually entered data, like product ratings. The service providers aggregate, combine and enrich the information from different sources to add more value. The information flows can be direct or indirect. A direct information flow can go for example from thing to thing, from business to consumer or from consumer to a thing. A indirect information flow can go for example from thing to business through service provider or from business to business through a thing. The resulting customer relationships can be structured according to the information flows. They can be for example unidirectional, bidirectional or multidirectional. The most important thing is to create a win-win situation for all stakeholders involved in the information exchange. (Bucherer and Uckelmann, 2011:263-266).

As the IoT-enabled products become more and more commoditized, businesses are forced to find new ways to create and capture value. At the first stages, the IoT business models will most probably heavily borrow from existing business models but also novel business models start to emerge (see table 3.2). The following chapters introduce some examples of traditional business models converted for IoT-enabled products and also some novel IoT-based business models.

Traditional business model	IoT-enabled business model	Description
Freemium	Physical Freemium	The offering consists of basic and premium versions, where basic version is free and premium version is paid.
Add-on	Digital Add-on	Core offering is priced competitively but at the same time the final price is raised by numerous extras attached to the core offering.
Lock-in and Razor and Blade	Digital Lock-in	Customers are locked using vendor's products and services. The basic product is sold very cheaply or given for free and the consumables are sold for a higher margin.
Self-Service	Object Self-Service	Some parts of the value creation are transferred to the customer. In exchange the customer can buy the product or a service for a lower price.
-	Product as Point of Sales	Converts physical products to sites of digital sales and marketing services. The customer can consume them directly by interacting with the product, or indirectly via mobile app or web site.
-	Remote Usage and Condition Monitoring	IoT-object's ability to transmit data about themselves or the environment in real-time is utilized. Enables preventative error detection, usage monitoring, and inventory management.
-	Sensor as a Service	Utilizes the idea of collecting, processing, and selling sensor data for a fee. In this business model the products that generate the data are not in the central focus but rather the data itself.

Table 3.2: Evolution of business models. (Gassmann, Frankenberger and Csik, 2013; Fleisch, Weinberger and Wortmann, 2015).

As in the more traditional business models, also when considering the IoT-enabled products, the most basic business models are retail sales and product lease or subscription. In retail sales the device manufacturer uses its own money or raises financing to build products which are then sold to customers. The device manufacturer captures the value only during the sales transaction. The expectation is that the cost of manufacturing is lower than the revenue. In product lease or subscription, instead of selling the product to the customer, the vendor leases the product to the customer. (Fabode, 2016).

In IoT-products, the physical product is always linked to digital services, which forms a single whole. This union can alter the traditional business models. In Freemium business model the offering can consist of basic and premium versions. The basic version of the offering is free to the customer and the vendor hopes that eventually some customers will pay for the premium version. The basic version attracts high volumes of customers and the premium version - whilst attracting fewer customers - generates the revenue. (Gassmann, Frankenberger and Csik, 2013). In IoT domain, the freemium business model can evolve to Physical Freemium business model. In physical freemium business model some basic digital service are included to a physical product free of charge. At the same time more comprehensive premium digital services are offered for a extra charge. (Fleisch, Weinberger and Wortmann, 2015). An example of an Physical Freemium product is the Logitech Circle security camera. Basic digital services, like motion detection and short term cloud storage are free when the product is purchased. If the user wants better video quality, longer time cloud storage for the recordings or advanced features, like person detection or motion detection zones, the user has to buy a premium subscription.

In an Add-on business model the core offering is priced competitively but at the same the the final price is raised by numerous extras attached to the core offering. Customers can tailor the offering to their needs. In Add-on business model the customers usually end up paying more than they assumed. (Gassmann, Frankenberger and Csik, 2013). In Digital Add-on business model the physical asset is sold cheaply at a low margin and the customer can later purchase or activate different digital service for a higher margin. In the future, the Digital Add-on business model could be used for example in cars. The user could buy performance improvements, like more torque or horsepower, for a short time period or buy a one-time insurance policy when travelling abroad. (Fleisch, Weinberger and Wortmann, 2015).

In a Lock-in business model the customers are locked using the vendor's products and services. Changing vendor is made difficult for the customer and it would cause substantial switching costs. In the Razor and Blade business model the basic product is sold very cheaply or given for free and the consumables are sold for a higher margin. The basic product and consumables are usually technologically bound and protected with patents. (Gassmann, Frankenberger and Csik, 2013). In Digital Lock-in business model uses both Lock-In and Razor and Blade business models. Only the original components are compatible with the product. The digital lock-in business model could be used by creating a sensor-based digital handshake that can limit compatibility, prevent counterfeits, and ensure warranties. (Fleisch, Weinberger and Wortmann, 2015).

In a Self-Service business model some parts of the value creation are transferred to the customer. In exchange the customer can buy the product or a service for a lower price. This can be used especially for process steps that add little value for the customer but incur high costs for the vendor. This again can cause benefits and time savings for the customer. (Gassmann, Frankenberger and Csik, 2013). In the Object Self-Service business model the self-service no longer only refers to the customer. The IoT-objects can serve themselves. In the Object Self-Service business model the IoT-objects are able to place orders independently, without customer interaction. An example of a Object Self-Service business model could be a household oil heating system. The heating system could place an refill order automatically when the oil level in the tank drops to a certain level. (Fleisch, Weinberger and Wortmann, 2015).

Some of the more novel, IoT-enabled business models include Product as Point of Sales, Remote Usage and Condition Monitoring, and Sensor as a service business models. The Product as a Point of Sales business model converts physical products to sites of digital sales and marketing services. The customer can consume them directly by interacting with the product, or indirectly via mobile app or web site. An object itself can become a web shop, carry digital advertising and collect and transmit loyalty points. Early indications of this business model can already be seen in some of Amazon's products. By reading the barcode from the product with a mobile app a web site is opened where the same product, replacement parts, accessories, and consumables can be purchased. (Fleisch, Weinberger and Wortmann, 2015).

The Remote Usage and Condition Monitoring business model utilizes the IoT-object's ability to transmit data about themselves or the environment

in real-time. This enables preventative error detection, usage monitoring, and inventory management. Today, the required technology for this business model might still be too expensive for less valuable products, but as the IoT continues to expand and become more and more commoditized, the costs will diminish and make the application for this business model possible. An examples of Remote Usage and Condition Monitoring business model can already be seen in more valuable products, like laser printers. Brother for example offers leases for laser printers without any base leasing rate, only the actual pages that are printed are invoiced. The transmission of the usage data to the supplier provides the basis for the implementation of the business model. (Fleisch, Weinberger and Wortmann, 2015).

The Sensor as a Service business model uses the idea of collecting, processing, and selling sensor data for a fee. In this business model the products that generate the data are not in the central focus but rather the data itself. As the measurement data from the IoT-objects are no longer collected, stored, and processed for the use of just one application but instead for a larger number of applications, this business model becomes more relevant. One example of the Sensor as a Service business model is a company called Streetline. Streetline installs sensors on municipal and private property that detect vacant parking places. The company then sells the collected data to interested third parties. The collected data has different value for different users. The car drivers can use the data for finding free parking spots, while the city government can use the data for identify parking offenders. (Fleisch, Weinberger and Wortmann, 2015).

3.3 Conceptualization of IoT business opportunities

The previous chapters described the overall structure of the IoT and presented an overview of IoT business models. The architecture of the IoT affects the sources of value creation and lay the foundation for different business models. The evolving and emerging business models have an impact on the possible roles a company might want to take, when considering starting IoT business.

This chapter describes the key phenomena affecting the roles a company might want to position itself when considering commencing IoT business. Based on the key phenomena, a conceptualization of IoT business opportunities is presented. The conceptualization of the IoT business opportunities is

created through a framework which combines the possible roles and positions for a company to take. The framework is expressly described from the point of view of the target company. The creation of the conceptualization of IoT business opportunities is based on three distinct phenomena, servitization of manufacturing, platform economy, and ecosystems.

The current global economy forces manufacturing companies to adapt to an ever changing business environment. Rapidly changing business environment has created trends, such as the servitization of manufacturing. Servitization refers to a tendency of a manufacturing company to expand their tangible, product-based offering with intangible services. Servitization term was put forth by Vandermerwe and Rada (1988) to describe the increased move towards offering more comprehensive packages of goods, services, support, self-service, and knowledge by companies. Other, closely related concept to servitization is the product-service system (PSS). Product-service systems are a type of value proposition that a business offers to its customers. Product-service systems consists of tangible products and intangible services combined in a way that the whole fulfills the customer needs (Tukker and Tischner, 2006:1552).

Service-dominant (S-D) logic is a theory that is derived from a analysis made by Vargo and Lusch (2004a), which illustrates the impact of non-manufacturing development of global economies. Service-dominant logic presents a new dominant logic, where service provision, intangible resources, value co-creation and relationships form the new fundamental base for economic exchange rather than the exchange of goods. The traditional economic worldview, the goods-dominant (G-D) logic, bases the worldview on manufacturing and tangible goods or products. The goods-dominant logic has been gradually replaced by the service-dominant logic. In the goods-dominant logic the aim is to produce and distribute valuable resources, which then are consumed by the customer. Value is embedded in the production output and it is determined by the producer. The ownership of the goods or products transfers to the customer in exchange and the customer then consumes, or, destroys the value embedded in the product. In the service-dominant logic the aim is to offer a value proposition and co-create value together with the customer. There isn't necessary a transfer of ownership. The value only emerges when the customer uses the service and the customer also at the same time co-creates value when they integrate their own resources with the service providers resources. (Vargo and Lusch, 2004a; Vargo and Lusch, 2004b; Lusch, Vargo and O'Brien, 2007).

There are many reasons, why a company would want to servitizise their product-based offering. The main motivators for companies seem to be financial, strategic, and marketing based. In financial perspective, servitization can stabilize company's income and contribute to higher profit margins. In strategic perspective, servitization can aid in gaining competitive advantage. In marketing perspective, servitization can help in creating stronger relationships with the customers. (Baines et al. 2009:562). The enablers that help in successful move towards servitization include technology, development tools and service-oriented viewpoint. Recent advances in IT-technologies has generated new opportunities to create better services and solutions. Different types of development tools can help in planning and creation of new services. Finally, the way that a company considers its products and services in relation of the customer has a major impact on the implementation of services. (Thornberry, 2017:45).

It is commonly agreed that ICT-technologies are the major driving force behind the progress of today's service world. Digital technologies, such as IoT, machine learning, cloud computing, predictive analytics, additive manufacturing, big data and many others are radically changing the way services can be delivered and it seems to crucial for the manufacturers to adopt these technologies when moving towards more service-based business models. Rymaszewska, Helo and Gunasekaran (2017:97) present ten strategic choices (see table 3.3) for companies aiming to include IoT in their product-service strategies. For the company to be able to determine their overall strategic positioning, they need to address the trade-offs between the choices. (Paschou et al. 2017).

Issue	Implication
Selecting smart capabilities	Continuous addition of capabilities may lead to blurred strategic differences and the creation of zero-sum competition.
Embedding functionalities: product and cloud	Embedding functionalities to the product will increase the overall costs of every product.
Open vs. closed system	Closed systems can create competitive advantage by allowing a company to control and optimize the design of all parts of the system relative. Open systems can enable faster application development and system innovation as multiple entities contribute.
Development of capabilities performed in-house or externally	Companies should seek a balance between developing certain layers of technology in-house while simultaneously outsourcing certain capabilities.
Data to be captured, secured and analysed	Maximizing the value of an offering will be affected by the decisions regarding product data. The investment in, for example sensor technology and the amount of data collected will affect to successful implementation of the IoT-powered servitization.
Ownership and access rights to product data	Certain restrictions should be considered as data becomes a valuable commodity.
Full or partial disintermediation of distribution channels or service networks	Better knowledge of customers can reduce the need for intermediaries and service partners. Companies need to plan how to address the changing customer proximity.
Business model change	Changing value propositions can lead to the existing business models becoming obsolete and uncompetitive.
Entering new markets by monetizing product data through selling it to outside parties	Capturing product data might open new opportunities for profit generation. Monetization of product data presents many problems, for example, whether the data should be available to entities that have no connection to the products.
Expanding company's scope	Connected products become part of a bigger product systems and systems of systems, and therefore an opportunity for expanding the scope of the business will need to be addressed at some point.

Table 3.3: Issues and implications of IoT-powered servitization of manufacturing (Rymaszewska, Helo and Gunasekaran, 2017).

Table 3.3 summarizes the issues and the implications they cause when building a strategy that is based on IoT-powered servitization of manufacturing. Finding solutions to each strategic issue can help companies in building servitization strategies that are based on the IoT. It seems that IoT-based solutions can serve as considerable tools for building product-service systems in the future. Some of the value-adding offerings presented by the IoT-based servitization include predictive maintenance, warranty modelling, consumption control, energy savings and customized utilization of the product. Also, completely new billing systems can be introduced to concepts that are based on a "as-a-service" models. These include concepts like SaaS, PaaS and MaaS (Software-, Product-, and Machine-as-a-service). These new billing systems can be based on, for example on the equipments efficiency or actual

rate of usage. (Paiola, 2017). The transition from manufacturing towards services presents also challenges for companies. Table 3.4 summarizes the main challenges that servitization generally presents.

Challenge	Description
Leadership support	Leadership support needs to be created throughout the company, from top management to sales and operations management.
Finance	Necessary investments need to be made in order to develop and implement services and solutions.
Change in mindset	mindset and capabilities of the organisation needs to be changed for it to be able of selling and delivering services and solutions.
Capture potential	Strategic effort is needed for being able to capture the potential of the installed base.
KPIs	Key performance indicators need to be agreed and incentives aligned to ensure integrated sales and delivery of products combined with services.
Development	The development of new products integrated with new services needs to be coordinated.
Customer involvement	Customers have to be involved in the development process.
Flexibility and adaptability	Necessary flexibility and adaptability to enable customization needs to be created and supported.
Value propositions	Attractive value propositions through better understanding of customer needs needs to be created.
Quality of service	Quality of service provision has to live up to the customer expectations.
Risk management	Service level agreements needs to be created and agreed for ensuring an appropriate balance of risk and rewards in the face of information asymmetry.
Relationships	Trustful relationships to support the investment in customer specific competencies needs to be created.
Distance management	Geographical and cultural distances in a globally distributed network of service partners needs to be managed.

Table 3.4: Challenges to servitization (Avlonitis et al. 2014).

In addition to the servitization challenges presented in Table 3.4, servitization based on the IoT creates some unique challenges. As the Table 3.4 describes, the transformation towards service revenue models can cause financial challenges. Especially when the servitization is based on the IoT, the financial challenges can force companies to build ecosystems with partners and other manufacturers. Servitization also deepens the collaborative relations with the customer and the complexity of the IoT-based services can create for example contractual difficulties (Paiola, 2017).

The second phenomenon influencing the conceptualization of IoT business opportunities is platform economy. Platforms can be defined in several ways.

In their core platforms are environments, either technical, like software systems or physical, like places or goods, connecting different actors that derive value from others that participate in the platform (Church, 2017; Van Alstyne, Parker and Choudary, 2016). These different actors consists of the platform owner, users, and complementary business partners, often called complementors, which all utilize and benefit from the platform's base functionality (Suarez and Kirtley, 2012). Platforms can also be seen from different theoretical perspectives: through economics, which sees platforms as multi-sided markets, or through engineering, which sees platforms as technological architectures (Gawer, 2104).

Multi-sided platforms can be defined as technologies or products or services that enable direct interactions between two or more participant groups for primary value creation. Each of these sides are also affiliated with the connecting platform (Hagiu and Wright, 2015). Some examples of multi-sided platforms are for example Android, which connects manufacturers, application developers and users, eBay, which connects buyers and sellers, and Sony Playstation, which connects game developers and users. (Hagiu, 2013). There exists a plethora of platforms, ranging from physical platforms, like malls that link consumers and merchants, or newspapers that connect subscribers to advertisers, to modern digital platforms, like Google, Facebook, eBay, or Uber.

Value creation in perspective of platforms happens as the platforms act as conductors between two or more categories of customers that wouldn't have been able to connect or transact without the platform. Value is created when the platform coordinates these groups of consumers. The value for the customer, as well as the platform owner, increases with increasing customer bases, which is a phenomenon called network effect. (Gawer, 2104).

Network effects can be defined as a concept, where the value of a product to a consumer changes as the number of the users of the product changes (Liebowitz and Margolis, 1995). Network effects can be divided into direct, or same-side network effects, and indirect, or cross-side network effect. Direct network effect happens, when every adoption complements every other adoption. For example, a phone becomes more valuable to a user as the total number of phone users increases. Indirect network effects happens, when the arrival of an additional users creates a marginal effect to the seller and thus attracts additional sellers, and the total marginal effect of the additional sellers on the users can be attributed indirectly to the additional user. One example of indirect network effect can be seen in the gaming consoles. A

PS4 becomes more valuable as the variety of games increases, and this variety increases as the number of PS4 users increases. (Farrell and Klemperer, 2007:44; Clements, 2004:2). The impact that the network effects create to a platform are exponential rather than linear. The effect can be growth or decay, depending whether the network effects are positive or negative. Network effects also creates barriers to entry to others. Once many users, sellers or buyers, use a platform it becomes harder for rival actors to lure them away. (Hagiu and Rothman, 2016).

Today, many companies refer their products or services as platforms. There are some distinctions, that tilt a product or a system into being a platform. Even though a product or a system is extensible via APIs or plug-in architectures, it doesn't necessarily qualify as a platform. The key aspects that make a platform, circles around business models: how complementing partners are recruited, how applications and innovations are build around the product, and how value is created for all actors around the platform. (Algaze, 2016). Product companies usually begin by building devices or applications that often either enable some new activity, or makes some older activity more efficient. Platform companies usually start by building the core features and capabilities that are then packaged and incorporated into a product. Some examples of products are portable GPS systems and e-readers, both products, that were influential for some time, but eventually were replaced by smartphones. One example of a platform is Amazon. Even though the Amazon Kindle device became virtually obsolete when smartphones arrived, the Kindle application was still able to thrive because of Amazon's platform. In this perspective, it seems that often products do not exhibit long-lasting disruptive value, while platforms do. (O'Kelley, 2017). The key elements in a successful platform are related to how easily all participants can join the platform, how well does the platform attract new participants, and how well does the platform allow creation and exchange of value (Algaze, 2016).

A complete IoT system needs multiple components to work. An IoT system needs hardware, such as sensors or devices for collecting data and performing actions. An IoT system also needs connectivity so that the hardware can send the data to backend services for analysis. An IoT system needs also software that analyses the collected data and makes decision accordingly. Finally, an IoT system needs user interfaces so that the users can interact with the system. (McClelland, 2017). An IoT platform consists of the aforementioned components and so IoT platforms can be defined as platforms that manage the connectivity and interaction of the IoT devices, enable collection of device data, enable communication between company backend IT applications and

IoT devices, and enable developers to build software applications on top of the platform. A IoT platform can be seen as a central backbone for the IoT solutions. There are sometimes difficulties to differ a product from a platform and the same applies in the IoT domain. Sometimes companies call full stack IoT solutions IoT platforms, sometimes the so called platform can in fact be just one element of an IoT solution. But many times these solutions or elements of a solution built by companies that sell IoT devices are not for example open to anyone else in the market which makes it debatable whether they are platforms. (Hayes, 2016; Bui, 2016)

The third phenomenon influencing the conceptualization of IoT business opportunities is ecosystems. Many of today's digital markets require distinctive competitive strategies because the products are parts of a larger system that combines core components and form a platform made by one company, with complementary components made by variety of others. In some cases, a platform leader emerges that works with the other companies supplying complementary products and services. Together, they form a ecosystem that greatly increases the value of the platform leader and the complementaries. (Gawer and Cusumano, 2008).

The term ecosystem is used for describing a variety of concepts. The term is used for example to describe biological ecosystems, digital ecosystems, and business ecosystems. A biological ecosystem consists of an environment, and actors in it. A biological ecosystem environment is loosely coupled and domain clustered in nature. This means, that the actors join the ecosystem by their own choice and tend to form groups which share similar habits, interests and objectives. The actors use the environment in a self-organizing manner to interact and engage with each other and form a balance. (Boley and Chang, 2007).

Digital ecosystems can be defined as software systems that utilize the properties of biological ecosystems, like robustness, scalability and self-organization (Briscoe and De Wilde, 2006). A business ecosystem is a economic community that consists of interacting organizations and individuals. The ecosystem produces value to the customers - who also are part of the ecosystem - in form of goods and services. The ecosystem consists of suppliers, lead producers, competitors, and other stakeholders. Over time, the capabilities and roles of the actors in the ecosystem coevolve and tend to align with the direction set by one or more central actors. The central actor holding the leadership role acting as a ecosystem leader is valued by the other actors in the ecosystem. (Moore, 1996). A digital business ecosystem combines digital ecosystems and

business ecosystems with emphasis on the coevolution between the business ecosystem and the enabling technology of the digital ecosystem (Nachira, Dini and Nicolai, 2007:9). A digital business ecosystem offers a software environment which is shared, interactive, and self-organized and which can at the same time offer a unified view of all participating actors (Korpela et al. 2013).

Because of the vast amount of possibilities the IoT can offer and the rapid development speed of the IoT, it is quite impossible to give a definitive definition for a IoT ecosystem. The communication between a nearly countless number of devices resembles a natural ecosystem. The core software and hardware platforms, as well as the standards forming around the IoT, resemble digital platforms. The communities of interacting companies and individuals, acting within their socio-economic environment, utilizing a common set of core assets that are related to the interconnection of physical and digital world resemble a digital business platforms. (Rymaszewska, Helo and Gunasekaran, 2017; Mazhelis, Luoma and Warma, 2012).

The justification for creating a conceptualization of the IoT business opportunities which combines the possible roles and positions for a company to take is based on two facts. Firstly, the IoT is a difficult concept to define. It is difficult to create a comprehensive and common understanding on what the IoT is and what kind opportunities it has to offer. Secondly, the IoT is a complex phenomenon in terms of monetization. It is difficult to create a comprehensive understanding on where the real value of IoT can be created.

The creation of the conceptualization and the frame is based on three distinct phenomenon: servitization of manufacturing, platform economy, and ecosystems. In order to help determine possible roles which can be taken when considering IoT-based applications, the aforementioned phenomena are organized into a conceptualization (see fig. 3.7) in perspective of the domain of the target company.

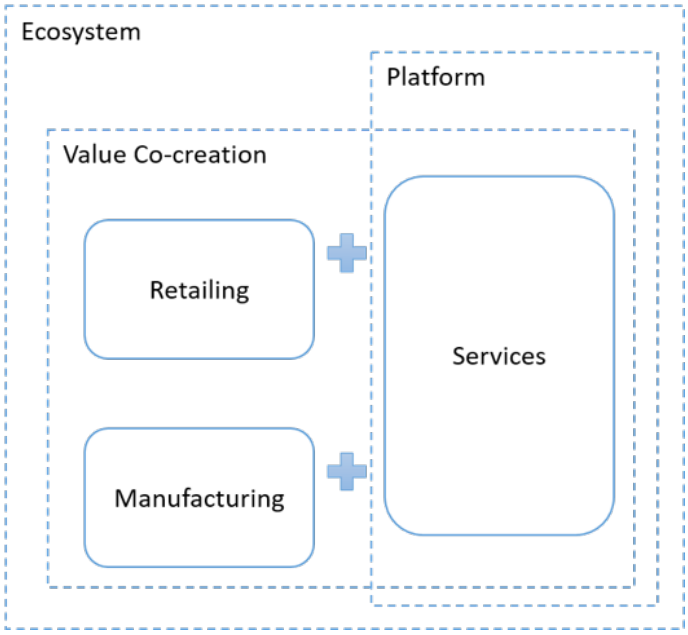

Figure 3.7: A conceptualization of the IoT business opportunities.

The basis of the conceptualization is on manufacturing and retailing of IoT-enabled products. In manufacturing role, companies can either manufacture their own IoT-enabled products or white label products can be used. In retail role, companies retail IoT-products manufactured by other companies. In these roles the possible services attached to the offering are not included. In manufacturing role the manufacturer doesn't include any services to the products. In the retailing role, the retailer doesn't have any role in the possible service offering the product may have.

As stated earlier in this thesis, the current global economy forces companies to adapt to an ever changing business environment. This can happen for example by moving more towards service business. Moving towards service business offerings holds many challenges and risks and requires lots of effort, so some companies might not want to move towards it. So some companies may decide on concentrating on their core business, whether it be manufacturing or retailing.

The services role can be included to both, manufacturing and retailing roles. In manufacturing role the manufacturing company can create and control the services created on top of the products. In retailing role the retailer can sell a combination of products and services, act as a service provider or a facilitator and participate to the creation of the service offerings in cooperation with

the manufacturing company, or create own services on top of the products and control what kind of services are offered as part of a product offerings.

When the manufacturer has the main responsibility of the services offered as part of the IoT-enabled product offering the manufacturer can make independent decisions on what kind of services are offered, what technologies are used, and who has access to the data created by the IoT-products. Although this may be worth pursuing in perspective of the manufacturer, it may lead to vertical silos, where the same type IoT products might not be compatible with each other. It might be difficult or impossible to gather data from different products even in a same domain because of incompatible technologies and data-usage decisions made by the manufacturers. This can then slow down or prevent the full realization of the potential of the IoT applications. When some other actor has the main responsibility of the service offering or acts as a facilitator creating a layer on top of the individual manufacturer offerings, the vertical silos can be avoided. Different technology choices do not create a substantial obstacles because of the extra layer created for combining data from different sources. Data-usage choices can be made considering the needs of multiple actors. This can then help in the full realization of the potential of the IoT applications.

As services are included into the product offering, a need for platform emerges. A 3rd party platform can be utilized or own platform can be created for the service offerings. The platform itself can be in control of the manufacturing role, the retailer role, or in control of a 3rd party. The owner of the platform can make the decisions on the openness of the platform. The platform can be made either internal, when only the owner has access to it, partially open, when some actor addition to the platform owner has access to it, or open, when all actors have access to the platform. Depending on the type and role of the possible platform, a possibility of a ecosystem creation emerges. The manufacturing and retailing roles can be an actor or a central keystone actor in the ecosystem. Again similarly as mentioned before, the owner of the platform or the keystone player in the ecosystem has a major impact on how the realization of the potential of the IoT applications will happen. The platform owner can make decisions, which leads to silos, or to an more open platform. Similarly, a keystone player in a ecosystem can make decisions, which can either help or hinder the needs of other actors.

This chapter described the key phenomena - servitization of manufacturing, platform economy, and ecosystems - affecting the roles a company might want to position itself when considering commencing IoT business. Based on the

presented phenomena, a conceptualization of IoT business opportunities was presented. The conceptualization combined all possible roles and positions for a company to take. The basis of the conceptualization is on manufacturing and retailing of IoT-enabled products. A services role can be included to both, manufacturing and retailing roles. With services included to the possible roles, a platform is many times needed. Depending on the type and role of the possible platform created, there is a possibility for a forming of an ecosystem.

3.4 Barriers of adoption

The previous chapter presented the overall structure of the IoT and business models that are forming around the IoT domain, as well as a conceptualization of the IoT business opportunities, which combined possible roles and positions for a company to take. All of those roles require different capabilities from the companies and create different kinds of challenges to companies and users. It is important to understand the challenges and risks that emerge when implementing and using new technologies. Because the IoT is a novel phenomenon, businesses have to cope with many different challenges and growing pains. Some of the challenges are in a way more general and apply to any other new technology as well, but there are also some unique challenges related to the IoT domain.

This chapter focuses on the technical, social, and business related challenges that companies and users can face when implementing and using IoT solutions, as well as presents needed capabilities for managing them. The technical barriers of adoption consists of challenges, like security, technical trust, connectivity, and interoperability. The social barriers of adoption consists of challenges, like privacy, ownership of data, and governance. The business barriers of adoption includes challenges related to monetization, financial impact, competence requirements, and business processes. The purpose of this chapter is not to create an exhaustive list of all possible barriers of adoption, but rather to create a overview of the most critical overall aspects that will be challenging when creating IoT solutions. The barriers of adoption are also not presented in any particular order of importance and many of the challenges presented in this chapter cannot be treated separately because they often contain complex interdependencies.

3.4.1 Technical barriers of adoption

The technical challenges related to the IoT consists of security, heterogeneity, trust, standardization, connectivity and interoperability, and data integrity issues, as well as challenges related to technology maturity, technical complexity, and power consumption. The overall security of the IoT is one of the main challenges and the nature of the IoT solutions expose them to both, digital and physical threats. The heterogeneous nature of the IoT environments creates challenges to technical trust management. The novelty of the IoT solutions and the lack of commonly accepted standards creates also challenges, especially to connectivity and interoperability. As the IoT technologies get more mature and the IoT devices become autonomous, the role of data integrity becomes more crucial and the risk on attacks against the integrity of the data increases. The technologies related to the IoT are still in a emerging phase and still relatively immature, but at the same time it seems that the nature of the IoT will force the technologies to evolve very complex. Finally, because the IoT devices will need to operate in places where continuous power supply is unavailable, there will be challenges related to the management of power consumption.

Security

Security in the IoT environment means securing the connected devices and the networks they use for transferring data (Rouse, 2015). The vast amounts of connected devices in the future will create completely new challenges for security. The highly distributed nature of the IoT and the use of novel and often fragile technologies can create weak links for exploitation. The IoT objects can face both digital and physical threats. Digital threats arise when the IoT objects are built without proper capabilities for software patches and updates, and when the IoT objects have to cope with limited processing power, making implementation of sufficient security measures difficult. Physical threats arise when the IoT objects are placed in public areas and unprotected zones, where they can be physically easily accessed. (Sicari et al, 2015).

The IoT environment consists of novel technology and communications stacks which can prevent direct use of traditional security countermeasures. The most major security challenges can be divided into three main areas: hardware, software, and communication. The need to use the IoT devices in environments where continuous power supply is unavailable creates challenges to utilize computationally expensive cryptographic algorithms for securing the IoT devices. Also, the IoT devices are usually built with limited memory

capacity, which is mainly used by the device operating system and system software. Traditional security algorithms are not designed to be memory efficient, which creates challenges for utilizing them in IoT devices. In addition, when the IoT devices are deployed in remote areas without sufficient supervision, they are more easily exposed for tampering. Physical tampering offers a possibility for extracting cryptographic secrets, modification of programs, and replacement of nodes which can be then used for attacking other devices. (Hossain, Fotouhi and Hasan, 2015).

The embedded software of the IoT devices needs to operate with limited processing and memory capacity. Because of this, the IoT devices need to operate on thin technology and network protocol stacks and there might not be enough capacity for sufficient security modules. Also, installing software updates or security patches to the IoT devices can be challenging. The operating system or the protocol stack of the IoT device may not have ability to receive and install new code or libraries, especially remotely. (Hossain, Fotouhi and Hasan, 2015).

The challenges related to the communication of the IoT devices are for example mobility, scalability, multiplicity of device and communication medium, multi-protocol networks, and dynamic network topology. Mobility is one of the main requirements of IoT devices. The IoT devices have to able to join a new network without any prior configuration, which can cause challenges for security. The number of IoT devices is growing in a rapid pace, and as the current security schemes lack sufficient scalability properties it will cause challenges in the future. Because of the diversity of the IoT devices, ranging from smart devices, like mobile phones to low-end devices, like simple RFID tags, it can be difficult to create any common security schemes. The same challenge can also be seen in the communication mediums. The IoT devices need to connect to many different networks. It can be challenging to find a common and comprehensive enough security protocol, that is suitable for wired and wireless communication. The IoT devices need the capability to use different network protocols. The IoT devices can use proprietary network protocols for communication in proximal networks and at the same time IP network protocols for communicating to service provider. This kind of multi-protocol communication can be very challenging when creating security solutions. Finally, the IoT devices need to be able to join and leave a network at anytime and from anywhere. This kind of dynamic network topology requirement can be challenging for existing security solutions. (Hossain, Fotouhi and Hasan, 2015).

There are many requirements that need to be taken into account when creating security solutions for IoT devices. The security requirements can be divided into information security requirements, access level security requirements, and functional security requirements. Requirements related to informations security are for example data integrity, information protection, anonymity, non-repudiation, and freshness. Data integrity means that it needs to be ensured, that data has not been altered in the transition. Information protection means that the secrecy and confidentiality of the communication and data storage should be strictly preserved. Anonymity means that the source of the data stays hidden. Non-repudiation means that an executed function cannot be denied. This means, that for example a IoT node cannot deny sending a message it has previously sent. Freshness means that the freshness of every message needs to be guaranteed. (Hossain, Fotouhi and Hasan, 2015).

Access level security requirements include requirements for authentication, authorization and access control. Authentication means that every IoT object needs to be able to identify and authenticate other objects. In the IoT environment, where multiple entities are involved, like devices, people, services, service providers, and processing units, there is a need to authenticate entities in every interaction. Authorization means, that it needs to be ensured that only authorized entities get access to network services and resources. Access control means, that the authenticated IoT entities are able to access only what they are authorized to and nothing else. (Hossain, Fotouhi and Hasan, 2015; Mahmoud et al, 2015).

Functional security requirements include requirements for exception handling, availability, resiliency, and self organization. Exception handling means that the IoT network stays alive and continues serving even if there is a anomalous situation. Availability means that the services can operate in and recover of malfunctions. Resiliency means that even if some IoT devices are compromised, the implemented security solutions still protects other devices. Self organization means that when some IoT devices in a network fail, the remaining network has the ability to reorganize and maintain required level of security. (Hossain, Fotouhi and Hasan, 2015).

Heterogeneity

As the IoT offers countless possibilities for companies, managing the numerous heterogeneous and constantly evolving IoT solutions can become a challenge. Many companies see business possibilities in the connectivity and

cloud-based applications that the IoT offers. This can create challenges in managing of heterogeneity in the product portfolio of the company. The heterogeneity increases as the number of product categories, product versions, and rapid and constant evolution increases. (Hackbarth, 2016).

Technical trust

The concept of trust is used in various different contexts and with different meanings. (Sicari et al, 2015). Trust in context of the IoT can be distinguished between different types of trust. The first type is behavioral trust, which looks at the expectations to the behavior of a participant. Behavioral trust is discussed in later parts of this thesis. The second type is computational trust, which usually happens in machine-to-machine interaction. Computational trust looks at the human notion of trust in the digital world. The third type is technical trust, which usually happens in machine-to-machine interaction. Technical trust looks at the establishment and evaluation of trust chains between devices. (Leister and Schultz, 2012:32). This section discusses about the technical trust aspects in the IoT environment.

Technical trust can be seen as the unifying factor that ties together the IoT devices and the technological ecosystem. It expresses the level of confidence that can be granted to the IoT device by the environment. The heterogeneous nature of the IoT environments can create challenges when defining trust management operations, like for example establishing, updating, and revoking keys and certificates. (Riahi et al, 2013). Some examples for trying to solve the issues related to trust management in the IoT environments include for example trust level assessment, trustworthiness evaluation, and secure distributed ad hoc network.

In the trust level assessment, it is assumed that most of the IoT devices are human-carried or human-related. This makes them often exposed to public areas and they communicate through wireless networks, which in turn make them vulnerable to attacks. The trust level assessment uses attributes, like friendship, ownership, and community for assessing the trust level. Hence, the trust management is distributed, encounter-based, and activity-based. The IoT devices that come in touch with each other or are involved in interaction can directly rate each other and exchange trust evaluation about other devices. That way they perform indirect rating about each other. The IoT devices can utilize reference parameters, like honesty, cooperativeness, and community interest for evaluation. This creates a dynamic trust management protocol, that can adaptively adjust best trust parameter setting in response to a dynamically changing environment. (Sicari et al, 2015).

In the trustworthiness evaluation, social networking concepts are used in the IoT environment. In the trustworthiness evaluation, the IoT devices are capable of establishing social relationships in a autonomous way. It builds upon the same idea as in the peer-to-peer networks, where each IoT device can compute trustworthiness of other devices based on its own experience and the opinion of other common devices. In a result, a IoT device can choose a provider of services it needs based on the highest computed trustworthiness level. The challenge in trustworthiness evaluation is to build a reputation-based trust mechanism which can effectively handle malicious behavior aimed to mislead other IoT objects in order to lead the use of services and information delivery only towards trusted devices. (Sicari et al, 2015).

The secure distributed ad hoc network is based on direct peer-to-peer interactions and communities creation. Each IoT device and community will have a identity in the network and they can modify the trust of other nodes based on their behavior. This creates a trust chain among the entities. The secure distributed ad hoc network uses parameters, like physical proximity, fulfillment, consistency of answer, hierarchy on the trust chain, similar properties, common goals and warrants, history of interaction, availability, and interactions. The created chains of trust allow creation of groups or communities and unique identities for the communities, which then helps granting access rights to services. In other words, the security and trust is established when the user access the services through the use of trust chains generated by the devices. (Sicari et al, 2015).

The traditional access control models will most probably not be suitable for heterogeneous, decentralized, and dynamic IoT environments, where identities are often unknown in advance. Trust relationships between the IoT devices can be utilized for helping interactions. When devices can technically trust each other, sharing of resources and services becomes possible. As it can be seen from the previous examples, there are many different techniques emerging for handling the trust management challenges in IoT environments. But still it seems, that a common definition of fully distributed and dynamic approach that is suitable for IoT environments is still missing. There is still need for a well-defined trust negotiation language that supports the semantic interoperability of the IoT, a need to define a proper object identity management system, and a need to define adequate trust negotiation mechanisms. (Sicari et al, 2015).

Fragmented standards

As the IoT disrupts many industries, and the number of IoT solutions grows in a fast pace, the risk of mass fragmentation rises. Companies many times want to develop their solutions with technologies best suited for their situation. This can lead in to a situation where some parts of the solution, like security, is poorly designed and the used technologies might prove to be wrong. There are also signs, that if common standards for the IoT are not found, the evolution of the whole IoT ecosystem might become difficult. The fragmentation of the IoT ecosystem does not only affect businesses, but also consumers. If businesses use different technologies when building their solutions, cooperation becomes difficult. Interoperability challenges reduces the usefulness of the IoT devices and makes the utilization of the devices more difficult for consumers. (Fearn, 2017).

Connectivity and Interoperability

While IoT devices in consumer space are relatively easy to connect and they can be, at least to some extent, interoperable, the connectivity and interoperability of IoT devices face far more difficult challenges in the industrial IoT implementations. In many companies it is commonplace to utilize decades old legacy systems. These legacy systems still offer value for years to come, and they can be difficult to connect with novel IoT systems. The IoT systems in industrial environments need to support numerous different vendors and standards, and they need to be able to scale to vast amounts of devices and data. (Sookne, 2016; Forbes Insights, 2017).

The connectivity and interoperability challenges of IoT devices, especially in industrial environments, are related to difficulties integrating new technologies to existing environments, difficulties in managing complexity, lack of standards, lack of best practices, different organizational attitudes towards change, and data management issues (Sookne, 2016; Wasserman, 2016; Forbes Insights, 2017). In the consumer environment, there are numerous competing technologies fighting for dominance and standardization remains elusive. Industrial environment is even more complicated and replacing working systems can be technically and economically difficult to justify. Many times retrofitting is the only viable solution for bringing IoT capabilities to existing systems. Adding IoT capabilities to existing systems can offer potential for big benefits, but the implementation can be very difficult, laborious and costly. (Forbes Insights, 2017).

Managing the complexity related to different IoT protocols can also create challenges. There are many different IoT specific protocols, like BLE, ZigBee,

Z-Wave, and Thread that are quite similar, but differ for example in operating radio frequency, operating range, and number of supported devices at same time. The number of IoT protocols is extensive, each having their advantages and drawbacks. Previously the core systems of a company might have been tied to a single vendor, but in the future the systems have to be able to work with numerous, often rival, vendors and systems. As there is no single common standard for the IoT, companies have to choose the protocols and technologies in a way that they are compatible with the core platform and that the protocols and technologies can be changed as the standards evolve. (Wasserman, 2016; Forbes Insights, 2017).

Best practices in the IT field can be defined as procedures that are commonly known and accepted being most effective. Best practices help in writing code, managing lifecycle, and handling of unique problems that can occur during development. As the IoT implementations are novel, the best practices are yet to be formed. As the IoT continues to evolve, there will be some growing pains which will help in creation of best practices, but this will take time. There will also be challenges related to different attitudes about change of technologies. The people responsible of the core operating technologies of a company make decisions based on different requirements than people responsible of IT development. The core systems are selected to operate for decades, while some other systems can be replaced or updated as soon as something better comes up. (Sookne, 2016; Forbes Insights, 2017).

The challenges do not end when connectivity and interoperability has been established. The IoT solutions create possibility to collect vast amounts of data. This can create a challenge if the infrastructure cannot handle the data efficiently. Companies have to make decisions on how they will manage vast amounts of data while staying at the same time somewhat agile and avoid data floods. (Sookne, 2016). New standards, protocols, and connectivity options will become more prevalent in the future. Companies have to make sure that new technologies remain compatible with legacy systems and processes (Forbes Insights, 2017).

Data integrity

As the IoT technologies get more mature, they allow more and more efficient gathering and analysis of data. At the same time, as machine learning and AI solutions become more and more efficient, the IoT devices are able to become more autonomous and start also doing rather just sensing. The IoT devices are able to not only collect data, but also to analyze it and adapt its behavior,

without any human input. In the more traditional IT solutions, stealing of the data has been the major risk, but in the IoT solutions there is another major risk, the risk on attacks against the integrity of the data. Corrupting the data that the IoT device utilizes can cause it to act in unwanted ways. There are numerous problems that the manipulation of data could cause to IoT devices. There are many solutions being developed for preventing possible issues with data integrity, like blockchain. Decentralized verification mechanisms can be used for ensuring the veracity of the data. But as in many security solutions, it can be difficult to scale the solutions up fast enough to be able to drive safe development of IoT solutions. (Gaillard, 2016).

Technology maturity and technical complexity

The IoT technology is still in a emerging phase and still relatively immature. The technology immaturity creates risks in the architecture and development of IoT solutions. At this point, there are no dominant ecosystems available. Security for example remains a big challenge until vendors, consumers, and IoT devices are mature enough. The immaturity can also be seen in the business model innovation. Vendors seem in many places promote subscription type business models. Subscription type business models have been in use in the B2B side for a longer time and it is more familiar model for businesses, but it seems to be also slowly spreading into B2C side. (Gonzales, 2018).

The possibility to measure, monitor, and control any device and its environment are the main benefits a IoT solution offers. To enable such functionalities, the IoT solutions evolve to be very complex. For example, a car of today consists of tens of thousands smart parts. These parts generate about a GB of data per second when in operation. All of that data needs to be captured, managed, and used efficiently in order to be able to support data driven decision processes. A IoT solution must support the whole lifecycle of the data, from sensing to analysis and action, in a heterogeneous environment. At the same time, security of the data and the network needs to be ensured. (Upadhyay, 2017).

Power consumption

The IoT devices performing the sensing or actuating need power to operate. In many cases, the IoT devices need to work without continuous power supply, relying on a battery which practically cannot be changed, or rely on power harvested from the environment. In addition, the IoT devices usually require a long lifetime. Together these requirements can create challenges for the power consumption of the IoT devices. (Blaauw et al, 2014; Chen, 2012).

As the design requirements for IoT components seem to be small size and low cost, but yet sufficient functionality, and when the hardware and data transmission requirements vary widely, the sleep mode and active mode power consumption requirements of the components are difficult to fulfill. The sleeping time of the IoT components is usually many times higher than the active time. The leakage power of the IoT components should be kept at minimum, which is difficult especially when using more advanced components. Low active power consumption is also a challenge, especially when aiming for lower costs. Lower costs usually equals to lower performance and longer process latency and longer process latency causes higher power consumption. (Chen et al, 2014).

Trying to cope with the power consumption requirements of the IoT devices can also escalate other challenges related to the IoT. Minimizing power consumption can lead to for example security vulnerabilities, if some security functions are not implemented in order to minimize power consumption. Also, power consumption optimization can prevent the intended utilization of the IoT device. For example lower reading or transmission frequency of sensor data may prevent detection of malfunctions immediately when it occurs.

3.4.2 Social barriers of adoption

The social challenges related to the IoT consists of lack of common understanding, privacy, trust and data ownership issues, as well as challenges related to the governance and ethics of the IoT. Creating a common understanding about the IoT will be crucial for the realization of the benefits that it can offer. Challenges related to the privacy of the IoT can be seen as one of the major issues. As the privacy requirements in the IoT environments are not currently covered sufficiently, there is a need for well-defined privacy policies. Behavioral trust is another topic, that will create major challenges. The users need to able to trust, that the IoT solutions will do what they are supposed to do, without bringing harm to the user. As the IoT will present a completely new world when considering the rights and protection of individuals, completely new governance mechanisms and ethical guidelines are needed.

Common understanding

Creating a common understanding about matters, challenges and solutions between different actors in the IoT field is crucial in order to achieve the

benefits that IoT can offer. Building of common understanding starts with a clear and unambiguous definitions. After the definitions have been set, principles and frameworks need to be created. If the common understanding is not created, it will be very difficult to build ecosystems, frameworks, policies and relations that understand, interact and interoperate with each other. (Van Der Wees, Breeuwsma and Van Sleen, 2016:221-222).

Privacy

Privacy in context of the IoT, can be defined as the considerations required for protecting the information of individuals from exposure in the IoT environments. This includes the technical means of protection, as well as the ability for individuals to control the degree of interaction with the environment, including how much the individuals are willing to share information about themselves to others (Kumar and Dhiren, 2014:24). In the IoT environments, virtually any physical or logical entity or object can be identified uniquely and they have the ability to communicate autonomously. As these individual objects can transmit data autonomously they can also work together with other objects and form a smoothly working network of objects. The data gathered from one object may not create privacy issues, but when the data from a network of objects is gathered and analyzed it may form a sensitive information. (Rouse, 2014).

One of the most worrying and potentially dangerous part of the privacy issues in IoT environments is that currently the consumers are unaware of what kind of data is collected about them and how the collected data is used. As the current devices are slowly replaced by connected devices, consumers have less and less ability to buy devices that cannot track them and collect information about them. Users seldom read the privacy policies of the devices they buy or apps they download and even if they attempted to do so, they are usually written using legal jargon, which is hard to understand as an average consumer. (Bannan, 2016).

Typically the subject, either human or device, engages the IoT environment in a following way:

1. the environment is sensed by the connected devices.
2. the subject interacts with the connected devices in its environment.
3. connected devices collect the information.

4. connected devices relay the information to the back-end services via available network.
5. back-end services analyze the gathered information.
6. back-end services disseminate the analyzed information back to the subject and possibly to third parties.
7. a service is provided to the subject by the connected devices in the environment according to instructions of the back-end services based on the analyzed data. (Ziegeldorf, Morchon and Wehrle, 2014; Kumar and Dhiren, 2014:25).

Depending on the location of the back-end services, the flow of the information can be either vertical, horizontal or a hybrid. In vertical information flow, the data is sent to a distant central back-end. In horizontal information flow, the data is processed locally, by the connected device or by distributing it across multiple connected objects. In hybrid information flow, the data processing is done as a combination of local and central data processing. (Ziegeldorf, Morchon and Wehrle, 2014). The privacy protection in IoT environments can be divided into four parts: privacy in device, privacy during communication, privacy in storage, and privacy at processing. Privacy of the individuals should be protected at every step while interacting with connected devices (Kumar and Dhiren, 2014:25).

For assuring privacy in the device, unauthorized manipulation of the hardware or software of the connected devices needs to be prevented. For example, a connected device might be reprogrammed to send the gathered data not only to the legitimate back-end service, but also to the intruder. Data reliability, non-identifiability and tamper-resistance are especially important when considering privacy in device. Privacy in the communication means the assuring of the data confidentiality during the transmission of the data. The most common way to ensure data confidentiality during the transmission is data encryption. Also, the devices should communicate only if there is a need for it. Privacy in the storage means the assuring of the data confidentiality during the storage of the data. Only the data that is truly needed, should be stored and the data should be available only when needed. Pseudonymization and anonymization of the data should be used whenever possible. Privacy at processing means the assuring of the data confidentiality during the analysis and processing of the data. Data should be used only for the intended purpose and data processor needs to have the user's permission for the processing of the data and distribution of the data to third parties. (Kumar and Dhiren, 2014:25).

Privacy requirements in the IoT environments are not currently covered sufficiently. The rapidly evolving, scalable and dynamic environment of the IoT needs well-defined privacy policies. Increased corporate transparency is also needed and it will act as a foundation for privacy in the IoT to be built. The increased corporate transparency could be achieved by industry self-regulation or governmental regulation (Bannan, 2016). Creating sufficient privacy requirements in early stages of the development will be one of the most important factors for creating public confidence for the IoT devices and the adoption of novel IoT systems. (Sicari et al, 2015:152).

Behavioral trust

Trust in context of the IoT can be distinguished between different types of trust. The first type is behavioral trust - usually a human-to-machine interaction - which looks at the expectations to the behavior of a participant. The second type is computational trust - usually a machine-to-machine interaction - which looks at the human notion of trust in the digital world. The third type is technical trust - usually a machine-to-machine interaction - which looks at the establishment and evaluation of trust chains between devices. (Leister and Schultz, 2012:32). This section explains the behavioral trust aspects in the IoT environment.

Trust is a complicated concept to define because it is influenced by many measurable and non-measurable properties. The concept of trust actually covers bigger scope than security or privacy. Trust relates to many other factors besides security, like goodness, strength, reliability and availability. Preserving user's privacy is one way to gain user's trust. (Yan, Zhang and Vasilakos, 2014:121). From the IoT point of view, trust can be defined as the expectation that a smart object will do what it is supposed to do, without bringing harm to the user. This includes the perception of being secure and that the user knows with whom he is interacting with, what is going on and that the user feels being in control of what's going on, and understands what services are involved (Leister and Schultz, 2012:31).

In order to realise the IoT vision, where virtually any object can be connected, user's must be willing to trust the devices and the communication that happens automatically. In the IoT environment, new devices will be deployed continuously and old devices will be upgraded continuously to perform new services. The IoT environment will be adaptive to user needs and it will most likely be adaptive towards threats in the environment. Typically in the IoT environment, the user cannot be fully certain about with which

devices they interact and they cannot know the identities of the devices. On the other hand, the user's are usually aware of the services they request and what type of devices they are interacting with. (Køien, 2011:496;502)

In the future, the IoT environment will be diverse. Some parts of the environment will be safe and well protected, and some parts will be hostile to the user. The problem will be that the owner, operator, and user of the IoT devices cannot necessarily know if the environment is safe or hostile. The same environment can also be safe to one party and hostile to another. The dynamic nature of the IoT environment creates a need to understand the varying threat exposure levels. The user's will have to dynamically adjust the level of trust based on monitoring, risk assessment and mitigation strategies. (Køien, 2011:502).

The realistic recognition and assessment of risks is not an easy task. While humans are well adapted to recognizing some types of risks, the abstract risks associated to computers and the internet are difficult to analyze. Also, analyzing the risk severity of abstract risks is difficult to humans. In the IoT environment, human users tend to trust commonly used devices and services, distrust seldom used devices and services and distrust devices and services perceived to be outside of the user's control. These perceptions can create a mismatch between the actual risk level and the trust in the device or service. (Køien, 2011:502).

Other aspects, that have influence in the user's trust in IoT devices and services are the deception and retaliation behavior, altruism, reputation, association and brand, and the functioning of the human brain. The deception and retaliation behavior refers to the ability to perform conscious deception and retaliation associated to human behavior. Deception and retaliation happens usually in interaction between humans, but it can also be applied to human-to-device interaction. If the users feel deceived by the device or service they will probably trust it less in the future. Distrust towards the device or service may lead to retaliatory behavior, like for example by attacking the reputation of the device or the service. Altruism, which is inherent in human beings, is something that intruders often utilize, when scamming and manipulating users. The intruders usually first build users trust by behaving honestly and then exploit the user after trust have been achieved. (Køien, 2011:502-506).

Reputation, association and brand are all decisive factors for trust. Reputation, whether it be good or bad, well founded or not, fixed or circumstantial,

matters. Association is also an important factor when it comes to trust. New or unknown devices or services are usually associated to something already existing, which will increase or decrease the level of trust. The association to, for example, a desirable brand also creates trust in users. The functioning of the human brain also plays a key role in the trust towards IoT devices and services. Trust is often based more on the emotional responses than rational thinking. Many scams rely on manipulating the users emotional responses. If the user has been strongly emotionally affected, even an conclusive reasoning may not alter the user's decision. What comes to the human trust towards devices, it creates a situation, where strong emotions will override knowledge. This means, that the users may trust or distrust a devices or service far more or less than objective knowledge would support. (Køien, 2011:506-507).

Ownership of data

In the future, the IoT will generate massive amounts of data and both, the users and the IoT systems, will rely on proper generation, transfer, storage, processing and provisioning of the data (The European Commission, 2016:12). Data generated by the IoT systems will pass through numerous different actors, but who really owns the data?

As the IoT grows, more and more devices will be introduced to the lives of individuals. The range of these devices will be vast, starting from personal smart devices and expanding to smart homes and entire smart cities. One primary function of these IoT devices is to collect data. Often this collected data is about, or produced by people. As this data is collected, many kinds of data ownership issues arise; who owns the data? Who should have access to it? How the data should be used? Is all data equal? (Mashhadi, Kawsar and Acer, 2014:159).

For reaping the full benefits of the IoT the free flow of data must be made possible. The free flow of data means, that the data can move across national borders and across different industry sectors. The data should be accessible and reusable for all stakeholders in an optimal way (Oettinger, 2016). The need for free flow of data raises numerous issues relating to the ownership of the data and the concept of data ownership seems to be one of the most controversial topic amongst the IoT community (The European Commission, 2016:20).

Today, it seems, that there is no clarity on who owns, or should own the machine-generated data or whether there should be a owner at all. There

are various different business models involved to different IoT devices and services and many different contractual arrangements exists today depending on the IoT device or service. These contractual arrangements lead to different permission for accessing, transferring or using the data by different actors in the chain. It seems that these different business models have led to arrangements, where the owner of the IoT device or the owner of the sensor is not always the owner of the data they generate. These arrangements can also lead to restrictions of data sharing to third parties and create service provider lock-in situations (The European Commission, 2016:20-21).

Today, most countries don't have laws, that specifically mention IoT devices. Often general privacy laws apply, which can be a challenge. For example in the past, U.S.-based companies could quite easily collect data from users in the EU if they were certified under a program called Safe Harbor (Talbot, 2016). But in 2015, EU declared Safe Harbor invalid (Court of Justice of the European Union, 2015).

Laws affecting the IoT devices vary very widely depending on the country. For example, in the U.S. there are federal privacy laws affecting, as well as laws that vary by state. For example, 31 states have data disposal laws and 47 states have security breach notification laws and some states even have very specific laws, like law about collecting data from internet-connected TV's, but the laws are not uniform. In U.S, there are also other specific laws regulating the data privacy, like for example the HIPPA for healthcare devices and the Children's Online Privacy Protection Act if the user is under 13 years old. The Federal Trade Commission has issued an best practices report for protecting user data, that is aimed at companies manufacturing IoT-connected devices. The report is not a binding law (Talbot, 2016).

In the EU, the EU Commission has passed the General Data Protection Regulation which will standardize data privacy laws across the EU (Talbot, 2016). The General Data Protection Regulation is effective from May 2018 (Court of Justice of the European Union, 2016). The GDPR will give the users better control over their personal data and stricter requirements for companies when building data protection into their products or services (Talbot, 2016).

In the future, data ownership issues can lead to obstacles in accessing data. The European Commission (2016:21) points out that in the future, for example public services may have to increasingly rely on access to privately-owned data. One example of this kind of need is the traffic management systems;

the effectiveness of those systems would be much greater if they had access to the data coming from privately owned vehicles. This raises the question, whether the access to privately-owned data used for public objectives should be guaranteed by law (The European Commission, 2016:21).

If the vision of the IoT is realized, virtually all appliances will be gathering data about you. Data generated and gathered by the IoT systems will pass through numerous different actors - the end-users that creates it, the manufacturing company whose devices collects it, the software businesses that processes it and the app maker that shares it - and all of those actors may want to claim rights to the data (Best, 2016).

One major challenge in the data ownership is creating trust between companies. The problem many times is about sharing enough, but not too much data between different actors in the value chain. One example could be a car manufacturer, who uses a smart device in their car build by another company. Because of this smart device, the car manufacturer can now track how often a certain part breaks down or need maintenance. The car manufacturer can also use the data from the smart device to other purposes, for example to enhance the assembly line work. Also the smart device manufacturer may want to have access to this data because it could be valuable for the company. Now, in theory, sharing the data would be beneficial for both actors; the car manufacturer can use the data to improve its cars and the smart device manufacturer could use the data to better understand the car manufacturer and in that way provide better products and services to it. But the car manufacturer may not want to share too much insight about its business processes. The smart device manufacturer could potentially obtain competitive intelligence, which it could then sell to other car manufacturers. Similarly, the car manufacturer could use the data obtained from the smart devices and ask some other smart device manufacturer to make a better one (Light, 2016).

The IoT also has some unique challenges, when it comes to the ownership and usage of the collected data. For example changes in terms of usage may be difficult in IoT environments. Compared to, for example the mobile app business, if the app provider wants to change terms of use they can just ask the user to approve the new terms of use. Now, in the IoT appliances - for example a smart home device - there might be no reasonable way to ask for the users approval for the new terms of usage (Best, 2016).

The IoT also presents some ethical challenges related to the ownership and usage of the data. Should for example a company manufacturing smart

dishwashers have access to usage patterns of the said devices? Or should they know what kind of detergent is used in the machines? If you drive through red lights with your car, is it ethical to provide this information to your insurance company, which can therefore raise your premiums? (Guinard, 2015). Should a smart home device manufacturer be able to determine from the data when you are home or how many people are in the house? Or should a smart TV be able to record conversations in the house?

Also the question, is all data equal in IoT environments is something that needs to be considered. Sensitive data, like health, finance and communications have to be subjected to strict privacy and security requirements. More general data, like data from wearable device or data about shopping preferences may be something that the users may be willing to share if it improves their customer experience. In this world, where everything becomes more and more connected, it will be essential that guidelines are developed for addressing the privacy and security concerns. It will also be important to educate the consumers to better understand the value of the data, and how and where the data about them is being used (Guinard, 2015).

There are multiple different models of data ownership either formed or forming in the IoT field. Mashhadi, Kawsar and Acer (2014:160-161) present three different models: Pay-per-use model, data-market model and open-data model. In the pay-per-use model users would only pay for the device based on the usage as the manufacturing company collects the data from the device. So the users would gain a monetary benefit from the data they share through their smart appliance. This model comes from the idea, that in the future, when appliances become more and more connected and aware of their current state and usage patterns, it can be hard to specify the usage of gathered data beforehand. The companies may want to use the data to interpret information about the usage beyond the original purpose (Mashhadi, Kawsar and Acer, (2014:161).

In the data-market model, the users are enabled to share their personal data for monetary benefits. The user would be able to trade with data with interested business entities e.g. data exchange companies. This kind of model of course opens up many privacy considerations. But it seems, that given a transparent framework and regulations, users would be willing to share their data (Mashhadi, Kawsar and Acer, (2014:161).

The open-data model relies on the concept of intention integrity, where users would be capable of wilfully access their data captured by public devices.

The data must only be used to achieve the intended operation and any other usage must be first approved by the user. The open-data model would answer the more bigger challenge, where the bigger picture of entire smart cities is viewed. For achieving the full benefits of IoT, it is important to be able to reuse the already deployed devices for purposes beyond their primary intention. The challenge in open-data model comes from the role identification; how are those who are affected by the device data collection identified? (Mashhadi, Kawsar and Acer, (2014:161).

The concept of data ownership, particularly in IoT environments, is a complicated issue. There seems to be no clarity on who should own the data or if there even should be a owner, and the situation will remain so for time being. Many different stakeholders have needs for the machine-generated data in IoT environments; private companies want to monetize the data, public sector want to utilize the data, and private users want to keep their privacy. The data is the lifeline of the IoT. On one hand, for the whole concept of IoT to work effectively, the data needs to able to flow freely across countries and across different industry sectors. And on the other hand, the privacy of individual user must be protected.

The data ownership issues, especially in IoT environments, will be needing regulations and governance for them to work in practise. If we want to one day achieve a true free flow of data across national borders, the legislations between different countries should be developed even more in collaboration. Also, the free flow of data between different companies and industry sectors will be needing some kind of regulations and governance so that conflicts can be avoided and trust can be created. Finally, all data in IoT environments may not be equally sensitive but the consumers must be able to rely that the sensitive data about them remains private and secure.

Ethics

Ethics can be defined as the moral principles which governs the behaviour of a person or the conducting of an activity. It deals with what is good and bad with moral duty and obligation. (Oxford Dictionary, 2017). Ethics in the perspective of ICT can be defined as the procedures, values and practices that govern the processes of consuming computing technology and its related disciplines without damaging or violating the moral values and beliefs of individuals, organizations or entities (Techopedia, 2017).

Traditionally the ICT domain has mostly been regulated through legal instruments. The ICT normative issues has been primarily identified with

privacy and data protection. Legal frameworks - consisting of hard and soft laws - have been built to take care of the concerns. Recently, also other relevant normative issues, besides privacy, have become apparent and specific roles for ethics have become more relevant. This involves especially the rapidly developing sectors, such as the IoT. (European Research Cluster on the Internet of Things, 2015:24).

The IoT will present a completely new world when considering the rights and protection of individuals. Completely new concepts are needed and the working notion of individual rights and public good needs to be extended and re-established. The need for conceptualization will vary. In some cases rights and protections of other domains can be utilized in the IoT domain. In some cases, the IoT will have major impact on the interpretation and consequences of existing policies and law, which need to evolve to adequately promote responsible behavior in the IoT environment. The IoT environment will also need completely new rights and protections. It might be impossible for example to give consent or opt out in some IoT environments. (Farrell, 2017).

Baldini et al. (2016:8) list numerous challenges relating to the ethics in the IoT environment: economic incentives for data protection of the user are not directed to the user, incomplete information on the consequence of data disclosure, too large information space about the consequence of data disclosure, psychological biases, trade-offs between businesses needs to collect and process data and rights to privacy, cost of implementing privacy enhancing or data protection solutions, accountability, online and offline identity, digital divide, conformance to regulatory frameworks, and support for dynamic context.

The economic incentives for data protection of the users are usually limited to businesses creating the IoT devices and services. Many times the user has an inadequate understanding about the consequences of disclosing data. This lack of information has an effect on every privacy decision. The complete set of needed information to make a rational choice can be so large, that the user may not be able to access a IoT service in an effective way. There can also be psychological biases, like for example, the perception of immediate benefits can have a negative impact in longer term. (Baldini et al, 2016:8).

Trade-offs between businesses needs to collect and process data and rights to privacy means, that there can be a tension between the market's need for data collection and in the protection of user's data. The cost of implementing

privacy enhancing solutions that ensures proper care in collection, storage, and retrieval of the data can also be hard to target. Accountability of the IoT devices and services regarding to the users privacy is another difficult thing to determine. The separation of online and offline information can also be hard and it can generate privacy breaches. Users today have a different set of capabilities in accessing the IoT devices and services. Depending on the level of technical proficiency, users have different perception about privacy risks. The definition, implementation and conformance to regulations in context of IoT is affected by two factors: the speed of the evolution of the IoT, which is usually a lot faster than the regulatory processes and the cost of altering the already deployed IoT systems and devices. The support for dynamic context means that the use of the IoT devices and services and the processing and storage of the personal data may change depending on the context of use. (Baldini et al, 2016:8-9).

The European Research Cluster on the Internet of Things (2015:29) propose some ethical guidelines for the IoT environment. Firstly, a separation between privacy and other ethical issues should be made. This is because privacy is widely regulated, opposed to other ethical issues arising from the IoT domain. Secondly, users knowledge should be increased, especially about the ethical use of the IoT. Thirdly, identity, autonomy, trust, human agency, social digital divide and increasing social isolation should be especially noted. (European Research Cluster on the Internet of Things, 2015:29).

Technologies have neither social values nor ethics. The same systems that can be used to make our lives better can also be used for misbehavior. The full potential of the IoT will only be achieved when we have a common sense of appropriate behavior, social mechanisms for enforcing responsibility and accountability. We also need to enable technical architectures which incorporate safety, security and protection. All of this needs to be developed in coordination now, when the technology is still novel. (Farrell, 2017).

Governance

Governance can be defined as the rules, processes and behavior that affect the way that powers are used, especially regarding openness, participation, accountability, effectiveness and coherence (European Research Cluster on the Internet of Things, 2015:13). Governance, in the perspective of the Internet, can be defined as development and application of shared principles, norms, decision-making procedures, and programs which shape the Internet's evolution and use. The execution of the development and application

is carried out by governments, private sector and civil society, all in their respective roles. (Almeida, Doneda and Monteiro, 2015:58). One interesting question about the governance of the IoT is that does the IoT need separate governance mechanisms, or are the existing Internet governance mechanisms sufficient?

The European Commission's public consultation on IoT governance (2013:11-13) shows, that there is no consensus on the need of separate IoT governance mechanisms. It is argued, that on one hand there is a need for a specific IoT governance, and there should rather be a one unified IoT than a multiplicity of IoT silos without interoperability. In addition, there is a need to define the IoT governance before IoT is widely deployed. On the other hand, it is also argued, there is no need for a separate IoT governance mechanism, since the existing Internet governance mechanism could be utilized (Weber, 2013:343). For the IoT governance model not to become too bureaucratic and slow, the IoT deployment should be governed by current horizontal regulation, like privacy rules and safety regulations. In addition, industry-led standards and general principles should be utilized. Also, at this point, it's quite unclear if there even can be a one unified IoT. The public consultation on IoT governance also shows, that the level of prescriptiveness of the IoT governance should mainly be soft, combined with strong self-regulation. On the other hand, crucial issues, like privacy and safety should be governed more strictly. Finally, the possible governance body for IoT should utilize multi-stakeholder approach, where public authorities, private sector and civil society are included.

The European Research Cluster on the Internet of Things (2015:13) argues, that the concept of IoT governance is the next logical step from the Internet governance. They argue, that the high number and heterogeneity of technologies and devices in the IoT actually requires even more specific governance than the Internet. Governance can be seen as a double-edged sword; it can offer stability and support for decision-making, and it can also become excessive and result in an over-controlled environment. Because of the many stakeholders and different positions, creating a common definition for the IoT governance is a difficult task. The European Research Cluster on the Internet of Things (2015:13) argues, that at this point, it is too premature to start policy development. It seems that there is no agreement on the special rules for IoT governance issues that are separated from other general rules. It is also possible, that the differences between the IoT and the Internet have been overestimated at the beginning. Nevertheless, there seems to be a need to conduct an analysis about the major governance issues of

the IoT, like legitimacy, transparency, accountability, and anti-competitive behavior. It is quite difficult to separate the concepts of governance, security and privacy in the IoT environment. Addressing privacy and security aspects in order to achieve trust probably need governance mechanisms too. (European Research Cluster on the Internet of Things, 2015:13-15).

3.4.3 Business barriers of adoption

The challenges related to the businesses implementing IoT solutions consists of monetization and financial challenges, long time to value, and uncertain demand of IoT solutions, as well as challenges related to competence requirements, business processes, scalability, contractual difficulties, and operating in multi-vendor environments. As majority of the IoT solutions will require significant investments and long periods of time for development, there will be difficulties in the monetization of the IoT. Also it seems to be quite unclear, how the IoT is going to improve the financial results of businesses. As many of today's IT projects, also IoT projects can take a long time. Also it seems, that the demand for IoT solutions in consumer and business sides varies significantly. In the future, the IoT will create a need for completely new skills, and when consumers become producers, there will be a need for new generation of digital experts capable of understanding both the new technologies and also the societal impacts of widespread adoption of these technologies. There are many differences when comparing IoT services to common enterprise services. Technical implementation, communication model, and the orchestration of services can be different which can cause challenges to existing business processes. Companies can also run into problems when they start to expand their IoT projects over time. Many aspects that are valid for the contracts in the ICT environment will be equally valid to the majority of IoT contracts, so the same challenges will also apply. Finally, todays IoT solutions almost never come from one individual vendor.

Monetization challenges

The who will make money and how will money be made with the IoT can be challenging question. Many IoT solutions will require significant investments and long periods of time for development. All of the cornerstones of the IoT, like ubiquitous connectivity and generation and analysis of data can present challenges for monetization.

The monetization aspect of the IoT is a difficult subject on several levels. Firstly, at the very core of the IoT is the connectivity between all of the

different smart devices. In this viewpoint lies an assumption that someone is willing to pay for the connectivity, which isn't free to establish. There are business models forming in the IoT environment, where the costs of the connectivity are burdened to one side of the deal. This is because one side supposedly offers value to the other side, albeit in many cases, the offered value can be unclear and argued. (O'Donnell, 2015b).

Secondly, another cornerstone of the IoT, the generation of vast amounts of data, which will be analyzed and then turned into meaningful insights can also be difficult to monetize. Creating a large amount of endpoints that gather the data may not be an area of meaningful profitability. What comes to the analyzing of the gathered data, on one hand, analyzing the data from the IoT devices and creating meaningful insights can be an arduous and difficult task. (O'Donnell, 2015b). On the other hand, creating a continuous revenue stream from the data can be as difficult (O'Donnell, 2015a).

Thirdly, the capability for a single company to create a complete IoT solution and turn it to a profit-generating business can be difficult. Today, many companies can offer some part of the solution, but companies capable of creating a complete end-to-end IoT solution are scarce. In addition, it is still quite uncertain that a completely self-created, platform-driven IoT solution will guarantee any success. Even if a single company controls the whole IoT solution, monetization can require complex business models. (O'Donnell, 2015b).

Other challenges relating to the monetization of IoT include the diversity of connected objects, the time that a innovation takes to mature into a product or a service, and the level of maturity of IoT ecosystems. In the future, virtually every object can have an online presence. It will be difficult to standardize the interfaces of all of the different objects, which in turn makes creating business models difficult. The IoT innovations today are still immature in many ways. Few IoT products have been standardized and modularized for wider usage. Modularization of the IoT objects is a key prerequisite for wider adoption of the objects. (Westerlund, Leminen and Rajahonka 2014).

The maturity challenge of IoT ecosystems means that the forming ecosystems can lack clearly defined underlying structures and governance, stakeholder rules, and value-creation logics. The early ecosystem can be a unstructured, chaotic, and open playground for the participants. Also, some required participant of the ecosystem might be missing. To be able to create new business

opportunities means, that new relationships in new industries has to be created which in turn takes time and can be managerially difficult. (Westerlund, Leminen and Rajahonka 2014).

The monetization of the IoT will need some concrete use cases and compelling value propositions. Lack of clear monetization possibilities can slow down the adoption of the IoT. Although some novel technical innovations, theoretical use cases and future concepts may suffice for some part of the early adopters, wider mainstream adoption of the IoT will require well-grounded products and services with clear business models (Wadhwa and Puri 2016).

Financial impacts

It seems quite clear that the IoT will offer business value and strong Return on Investment (ROI) opportunities in the future. Still, it seems somewhat unclear, how the IoT is actually going to improve the financial results of businesses. It seems that companies are aware of the potential that the IoT holds, but in contrast with consumer and public IoT, without actual and quantifiable improvements in financial outcomes, it will be difficult for companies to move forward with IoT investments. The two main ways of IoT deployments for companies are the platform-first approach and the use-case-first approach (Chase, 2016).

In the platform-first approach, a company-wide IoT platform decision is first made. IoT platform is the core of the IoT solution, which is used to collect, store, and analyze the data from myriad of different devices and to which other enterprise applications are integrated. The challenge of platform-first approach is that companies have to make significant financial investments with no clear view of results. The risk for companies is substantial in platform-first approach, because companies have to make enterprise-wide decisions about the IoT platform based on still evolving technology. And finally, IoT platforms are by definition incomplete systems, they need applications to be developed which again lengthens the ROI. (Chase, 2016).

In the use-case-first approach, the deployment of IoT solutions will start from individual business initiatives, which most probably will not be viewed as IoT initiatives. Instead, they usually focus on driving some specific business outcome. In use-case-first approach, the main goal usually is a quantifiable business outcome which the IoT solution supports. The challenge in use-case-first approach is that it can lead to dissimilar IoT systems being developed, which causes difficulties in enterprise architecture. (Chase, 2016).

Determining the total cost of ownership and return on investment in a large-scale or a wide spread IoT solution can be challenging (Matteson, 2017). The costs consists mainly of hardware, infrastructure, and application costs. A significant part of the costs of an IoT solution comes from hardware costs which means building the actual smart gadget. The infrastructure of IoT solutions usually consists of middleware, network, and storage. Middleware is the computer program, that enables the communication between different sensors and the application layer of the solution. IoT solutions usually need a highly scalable wireless network to function. IoT solutions also need some kind of storage solution, either cloud-based or data center, for storing the generated sensor data. Applications are used to connect the hardware to the infrastructure and for users to manage the smart applications. In addition to these costs, also possible product concepting and Proof of Concept (PoC) before the actual development, and possible marketing costs need to be considered. (Klubnikin, 2016).

Competence requirements

It is said, that obtaining mastery in a subject takes roughly 10 000 hours for an individual. Building an organizational competency is far more complex and it requires numerous components across the organization to work together, including people, processes, products, market knowledge, skills and effective communication. (Benson, 2017).

The trends that the IoT brings with it, like the emergence of new jobs requiring completely new skills, and consumers becoming producers, create a need for new generation of digital experts capable of understanding both the new technologies and also the societal impacts of widespread adoption of these technologies. (Kortuem et al. 2013:54). Challenges that individuals face in IoT field are related to the merging of the physical and digital realms and understanding of embedded systems. Also, there will be a massive increase in the number of connected devices, objects, sensors and actuators. These will require skills in understanding the sensors, networks, integrations, augmented intelligence and behavior, instrumentation, and communications technologies (Namiot, Sneps-Sneppe and Daradkeh, 2017). The increase in the amount and value of data will require data analytics skills. Also security, algorithms, programming skills, distribution and collaboration, and creative and collaborative design skills will be needed. (Kortuem et al. 2013:55-56; Stackpole, 2015).

Organizational challenges, that companies face related to IoT include lack of executive sponsorship, organizational misalignment, insufficient collaboration across departments, slow adoption to change, and inconsistent market

feedback (Cranford, 2017). Many times the evolution of organizational competence follows the Conscious-Competence model (Cannon, Feinstein and Friesen, 2014:176). The model consists of four phases; unconscious incompetence, conscious incompetence, conscious competence and unconscious competence. In the unconscious incompetence phase, the organization is unaware of its own incompetence. In conscious incompetence phase, the company acknowledges its own incompetence. In the conscious competence phase, the company acquires competency through shared effort. In the unconscious competence phase, competences becomes a second nature. The process of transitioning from one phase to next is the biggest challenge in organizational perspective. (Cranford, 2017).

Aspects worth considering, when building towards organizational IoT competency include obtaining IoT competencies in areas of digital innovation, technology, and business models. Also, developing and communicating a clear and actionable IoT strategy is important. Companies should start small and aim to easy wins for reducing business risk. Companies should also seek ways to standardize and reuse common components across business units and projects. The building of organizational knowledge should be started from outside in, by starting with outside help while simultaneously developing internal IoT competencies. (Benson, 2017).

Business process challenges

Enterprise systems of today use often some kind of service-oriented architecture. Business processes in these kind of systems are modelled as an orchestration of the underlying services. The integration of IoT to enterprise systems also requires the IoT resources to be service-enabled. (Haller and Magerkurth, 2011).

There are quite many differences when comparing IoT services to common enterprise services. Technical implementation, communication model, and the orchestration of services can be different. This is because of the dynamic nature of the real world to which the IoT connects. It requires flexible inter-service communication that can handle complex, and sometimes unexpected event patterns. In the IoT environment, locality is much more important. This regards the origin of the data delivered and where the service is executed. Also, in the IoT environment, the often real-time data flow has to be handled. This requires the ability to extract the relevant information and events from the data. Finally, the IoT services are often inherently unreliable. The delivered data may be wrong or it can suddenly become completely unavailable. All of these different properties have to be taken in account when modelling processes including IoT services. (Haller and Magerkurth, 2011).

Contractual difficulties

Many aspects that are valid for the contracts in the IoT environment are equally valid to the majority of ICT contracts. Such contracts can be difficult to understand for numerous reasons. They can be characterized by vague wording incorporated with excessive use of technical terms. They are often written with previous states of technological development in mind, thus not being entirely suitable for new technology. The contractual wording of European versions of original US contract sources can be reproduced verbatim. Noto La Diega and Walden (2016;13) argue, that IoT contracts are rarely drafted with EU law in mind. (Noto La Diega and Walden, 2016:3).

The multi-layered structure of the IoT environment can make it challenging to identify and interpret applicable contracts. The multi-layered structure of the market - also seen in cloud computing contracts - can make the contracts difficult to understand. This is not only for the customers, but companies as well. One reason for this can be the lack of awareness of all the actors involved. (Noto La Diega and Walden, 2016:3).

The vast amounts of data created by the IoT environment can impair pre-existing information asymmetry in consumer contracts to the benefit of companies. It can take the consumers and the contract formation process further apart from each other. It can further discourage consumers to read and understand contract terms before agreeing to them. Finally, it can lead to a situation, where businesses take even more advantage of the consumer ignorance and apathy by for example, including one-sided contract terms like unilateral amendment provisions or using terms that restrict consumers access to juridical process. (Elvy, 2013;1).

New technologies, like the IoT, not only address, but also produce new accountability demands. These new accountability demands can cause difficulties for human actors. In many domains, business entities need to give account of their actions and they need to demonstrate working control mechanisms and procedures for preventing any system of malfunctioning. While the IoT technologies can actually help in facilitating inspections and improve the adherence to accountability demands, it can also produce new issues of accountability. This is because of the IoT technologies are usually embedded in everyday objects and can be almost invisible to the user. (Boos et al, 2013;449).

It can be difficult to get a clear picture of the contractual aspects in the IoT environment. First of all, It can be hard to even define and understand

them. Secondly, It can also be difficult to get a clear picture of the contracts as a whole, because the contracts often claim to apply only part of the IoT device, while they actually impact on their operations as a whole. Finally, the contract can claim to apply to a single IoT devices, while in fact the affect a whole cloud of things. (Noto La Diega and Walden, 2016:3).

IoT contracts also generate dependencies. In the IoT environment the market power resides in the supply chain and can vary considerably, for example, from the retailer, to a software developer, component manufacturer, or cloud provider. Also, the end-users are usually dependent of the provider in the sense of being locked-into a contract, where there is no room for customization and interoperability and portability are very limited. The contract is accepted by using the product or service, and there usually is no room for customization either in the moment of contractual acceptance or when the terms change. (Noto La Diega and Walden, 2016:3).

Other business related barriers of adoption

Scalability, in the context of business IoT barriers, means the expanding of the IoT solution over time. Organizations can run into problems when they start to expand their IoT project over time. The company may be able to implement a IoT solution with a relatively small amount of devices in one location, but cannot scale the number of devices and locations (Lee, 2016).

As many of today's IT projects, also IoT projects can take a long time. The time to value can be considerably long. Starting from the initial idea and development of business case and leading to design and implementation and rollout, each stage of the process takes considerable amount of time and have their own challenges (Lee, 2016).

The demand for IoT solutions today can be many times very uncertain. In addition, the demand for IoT solutions in consumer and business sides varies. It seems, that the demand for IoT solutions in consumer side will remain uncertain and slowly emerging (Rebbeck, 2017). We most probably will not see a explosive emergence of IoT solutions, but rather the IoT will be more like a natural evolution of products. The IoT in itself might not be a significant source of value but it can create additional value to existing products and solutions, especially at the early stages.

The multi-vendor environments, in which the majority of today's development projects are done, can also present challenges. Today, IoT solutions almost never come from one individual vendor. The company's internal IT

department can be forced to learn functioning of tens of individual applications in order to get the business value out of the solution. Still, the end-users should see a unified IoT solution, easy to adopt and use, not a complex network of different components. (Novison, 2016).

This chapter presented the most important technical, social, and business related challenges that companies and users may face when implementing and using IoT solutions. The technical barriers of adoption consisted of challenges like security, technical trust, connectivity, and interoperability. The social barriers of adoption consisted of challenges, like privacy, ownership of data, and governance. The business barriers of adoption included challenges related to monetization, financial impact, competence requirements, and business processes.

Chapter 4

Case study implementation

Chapter three of this thesis presented a conceptualization of possible roles for a company to take when considering IoT business opportunities. The main objective of this chapter is to examine one concrete use case, smart water metering, in perspective of the created conceptualization of IoT business opportunities. This chapter consists of an overview of smart water metering field and an review based on the created framework. The review will examine the possible roles for the target company to take, what kind of barriers of adoption are related to each of the roles, what capabilities each role requires for the target company, and what kind of advantages are associated to each possible role.

4.1 Smart water metering overview and context

Water and wastewater systems are one part of the critical infrastructure of today's urban societies with other critical infrastructure, like roads and electrical networks. Digitalization has already started to affect other infrastructures and now it is slowly starting to transform also the water industry. A water distribution system of today handles the supply of water to end users through pressurized pipe networks. The water network can be built as loops or as a tree-like structure or a combination of the two. Wastewater systems are usually built in a tree-like structure, where the wastewater is collected from end users and directed to a wastewater treatment plants. (Cepa et al, 2016).

The water and wastewater network together with the treatment plants form the physical assets, which are owned and operated by the water companies.

The core services related to water and wastewater systems have been typically offered by the water companies, which in Finland are usually partially or fully publicly owned. The ownership and governance of these systems affect on the drivers and barriers for change in the industry. The water and wastewater systems are many times considered as a self-evident systems which are not considered until problems occur. The problems can be for example water shortages or flooding in the street or in a building due to water pipe breakage. The aforementioned problems can lead to a significant structural and environmental damage and costs. Water damages can be actually considered bigger threat to properties than fire damages (Partanen, 2013). The capabilities of IoT solutions can help in preventing such threats. (Cepa et al, 2016).

The water industry can be considered as a conservative field of industry. At the same time, the water industry has a lot of potential for digitalization and IoT solutions for example in form of collecting and utilizing data from the status of the network assets. The adoption and use of smart devices and services, which are common in many other industries, are still mainly missing from the water industry. The water networks can be considered quite data-scarce. One reason for this is the geographical extent of the networks. Today, the static datasets, like asset types, materials, dimension, and installation years, are stored in the companies internal systems. Online measurements are still rare and the connectivity between different datasets and between the data and actual network items are often missing. Another reason for slow adoption of new technologies and emergence of new services is the fact that the water and wastewater companies are natural monopolies. (Cepa et al, 2016).

The IoT devices, that could be utilized for better understanding of the networks include for example, pressure and vibration sensors, online water consumption meters, flow meters, and water quality measurement devices. As the water and wastewater networks are placed underground, the installation of extensive sensor networks to existing systems can be expensive and slow. Of course the installation of new pipeline materials equipped with sensors when repairing or replacing the pipelines is more cost effective. Even a relatively loose sensor network can drastically improve the understanding of the network functioning compared to current systems and as the IoT devices become more cheaper and data analytics more efficient, the investments can become profitable. Another way for starting collecting data is the household water meters. The smart water meters can measure water consumption and send the measurements to water companies. Smart water meters could offer

benefits similar to energy field, where the smart grid has been under active development for many years. (Cepa et al, 2016).

For understanding the digitalization possibilities of the water industry, it is important to understand the current business models of the sector. The business model describes the customer value proposition, cost and revenue structures, key resources and processes, key partners, key activities, and customer relationship. The value proposition of the water and wastewater companies is to deliver drinking water to its customers and collect and treat wastewater. The main customer segments are individual households, housing companies, industrial customers, public customers, and also sometimes other water companies. (Cepa et al, 2016).

The revenue streams consists of usage rate, basic rate, and connection fees. The usage rate includes both, the fresh water consumption, and wastewater removal. The fresh water is billed based on the price per litre and litres consumed. The price per litre remains constant regardless the amount consumed. Also the wastewater removal and treatment is billed. In Finland, it is assumed, that the wastewater quantity equals the water consumption, so only the water consumption is measured. The cost structure is divided into fixed and variable costs. Fixed costs consist of network and other fixed assets, like piping infrastructure construction, modernization, and maintenance. Variable costs consists of water treatment costs, both freshwater and wastewater, and other variable costs, like personnel expenses. (Cepa et al, 2016).

The key resources of the water industry can be divided into three resources: physical, organizational, and human resources. Physical resources consists of the physical piping infrastructure and water reservoirs. It is good to notice, that the water companies own the piping network up to the property line of the customers. In the property line, there is a water meter, also owned by the water companies. The meter measures the water consumption, to which the billing is based. The use of these water meters on every individual household is forced with regulations. The organizational resources consists of operational and technical knowledge, intellectual property, and customer base. As the water industry is a natural monopoly, the customer base is a particularly valuable resource. The human resources consists of the employees of the water company. Key partners typically consists of construction companies, the government, equipment suppliers, and service providers. Key activities consists of freshwater treatment, water supply, wastewater collection, and

wastewater treatment, as well as maintenance of the infrastructure and facilities, and billing activities. Customer relationship consists of delivery of service and billing. (Cepa et al, 2016).

The motivation for starting digitizing the water industry is in the change to improve operations related to technical efficiency, smoother workflows, and economics. The costs of maintaining and renovating the water networks are considerable. Optimization of the spend can be improved through digitalization. Optimization can be done for example, on asset life span, on optimization of maintenance activities, and on operation and control of the networks. Also, the risks related to environmental problems and network failures can be better managed. (Cepa et al, 2016).

The asset management has traditionally relied on retrospective analysis of data, which to some extent can enable characterization of the deterioration behavior of different pipe groups based on attributes, like pipe age, size, and material. Also, deterioration models and statistical models have been built to model the deterioration over time. These models can be useful, but they require high quality and availability of data, which so far hasn't been widely available. In addition, these models are not very effective on their predictive power to the future. Still, by analyzing large amounts of historical data, it has been possible to create estimations on how the structural conditions evolve, which is an significant improvement to previous decades when the condition of the underground pipelines has been practically unknown. (Cepa et al, 2016).

IoT solutions can offer new possibilities for asset management in the water industry. The first step would be to install sensors to the network. Also, a platform is needed for managing the collected data. Once the water companies have obtained sufficient amount of data, efficient algorithms are needed for analyzing it. The interaction between the water companies and end users have been quite limited. The IoT solutions could also be used for enabling the consumers to participate in the data gathering. Accurate data from the network can help in earlier detection of failures and malfunctions and online monitoring can enable faster reactions to possible problems. Also, as the amount of collected data increases, it will be easier to make better conclusion of the network, like for example the durability of different materials. In addition, as the spatial and temporal models improve, also failure prediction might become possible. (Cepa et al, 2016).

4.2 Modelling IoT business opportunities

In this chapter the different roles for the target company to take in the smart water metering business are identified and discussed. Firstly, the smart water metering environment is described and the possible actors identified. Secondly, the value proposition for the smart water metering is discussed. Thirdly, the different roles, barriers of adoption related to the roles, capabilities required, and advantages achievable for the roles are identified and described. The smart water metering environment (see fig. 4.1) consists of the water metering device, connectivity from the device to data warehouse, data storage, and components for analytics and visualization.

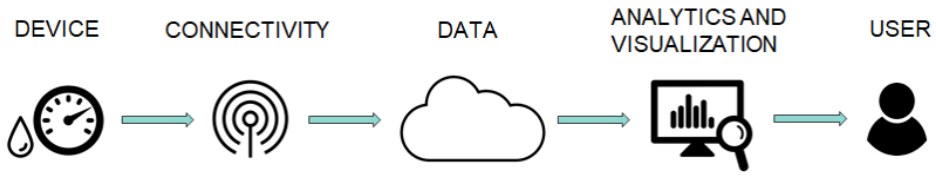

Figure 4.1: Smart water metering environment.

The IoT enabled device consists of the actual physical device, which in this example is a water meter device and sensors attached to it. The water meters can use different technologies for metering the water flow, based on for example ultrasonic or magnetic induction technologies. The sensors can measure for example the water flow, pressure, and leakage. The connectivity layer consists of different network protocols, which enable the communication between the device and back-end services. The data layer consists of different software components that enable the communication, provision, and management of devices, application platform, and software components that handle the storing of the sensor data. The analytics and visualization layer consists of different software components, that handle the processing and analyzing of the sensor data, software components that are responsible for the definition, execution, and monitoring of processes, and software components that enable the interactions between the users and the services.

The actors in the smart water metering environment (see fig. 4.2) includes device manufacturers, construction companies, regulators, network operators, IoT service providers, and users, like water service companies, consumer customers, housing companies, and insurance companies.

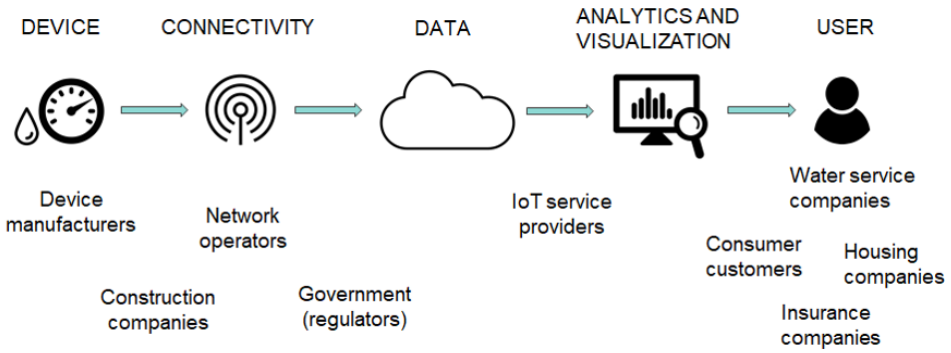

Figure 4.2: Actors in the smart water metering environment.

The device manufacturers offer the actual water metering devices. The device manufacturers can also offer the fully integrated IoT enabled smart water meters, including all required components, like sensors and batteries. The IoT capabilities can be also offered separately for existing mechanical water meters. Construction companies and service companies are responsible for installing and maintaining the devices. The regulators, usually governments, are responsible for various laws and regulations affecting the supply of water metering equipment and services. The network operators offer the communication infrastructure for the IoT devices. The IoT service providers offer the technical capabilities for data storage, analysis, and visualization. The IoT service providers can offer a ready platform that enables all needed capabilities or they can offer tailored solutions. The users in the smart water metering environment includes the water and wastewater service companies, who are responsible for operating the water and wastewater networks and treatment plants, consumer households and housing companies who consume the services that the water companies offer, and other users, like for example insurance companies.

For understanding the possible sources of value in the smart water metering case, it is sensible to do it by viewing the separate layers that form the IoT solution (see fig. 4.3). The layered value creation model is based on the model created by Fleisch, Weinberger and Wortmann (2015). In the IoT environment, the digital business model patterns mix with non-digital ones and form hybrid constructs. In this example, the IoT solution is divided into six layers: the smart water metering device, necessary sensors and actuators, connectivity, data storage, analytics, and visualization. The physical water metering device and attached sensors and actuators form the physical device. The data storage and the software components that are responsible for the analytics and visualization form the digital service.

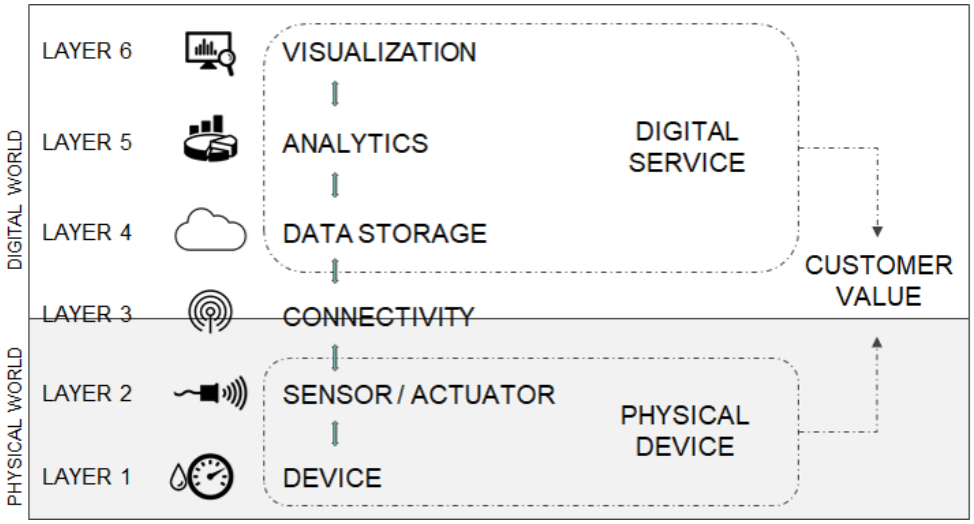

Figure 4.3: Value-creation layers in IoT applications (Fleisch, Weinberger and Wortmann, 2015).

The physical device, in this case the water meter, forms the first layer of the value creation model. It offers the first and most direct value to the users by measuring the water flow through the water meter. As the water meter is a physical device, it is always tied to a specific location and can only create value in its immediate environment, like for example in a single household.

The sensors and actuators that are attached to the physical device form the second layer of the value creation model. In layer two, the physical device is equipped with a computing unit, sensor technology, and actuating elements. These elements can be used for observing the physical environment and controlling the device either by the user or based on the collected data. With the sensor technology, the local data, like water flow can be measured. The actuating elements can be used for delivering local functions, like stopping the water flow in case of leakage.

Connectivity capabilities form the third layer of the value creation model. Connectivity enables the possibility to connect the sensor technology and actuating elements to the digital services through internet. This way the single smart water meter becomes globally accessible. The smart water meter device can transmit data to back-end services with a radio module, and the smart water meter can be accessed and controlled remotely.

The data storage forms the fourth layer of the value creation model. The data collected from the devices is sent and stored to a data storage. In the

data storage the data can be reviewed and grouped as needed. The data storage offers the necessary interfaces for accessing the data. In the smart water metering case, the interfaces can be used for offering the data to the water companies.

Analytics form the fifth layer of the value creation model. In the analytics layer, the collected data is analyzed in order to provide users with useful and interesting information. The data collected from the smart water meter devices can also be enriched with other relevant data. For example, the water consumption data used together with pricing information can be used for invoicing individual households based on the actual consumption.

Visualization forms the sixth layer of the value creation model. In the visualization layer, the capabilities of the other layers are combined and packaged to a suitable form and made available for users. The packaging can be for example a web service or a mobile application which is offered for the users. In the smart water metering case the visualization could mean for example a web service or a mobile application, which is offered for the households to monitor real time water consumption.

Smart water metering enables many improvements to existing business models and also enables many completely new business models. The improvements to existing business models include consumption-based billing, IoT-enabled asset performance improvement processes and differentiating pricing models. So far, the billing of used water has been based on an estimate which is checked at certain intervals. As the smart water meters enable real-time or near real-time metering of the water consumption, it offers the possibility to enable consumption-based billing for the users. Real-time metering of the water consumption also enables the digitalization and automatization of the meter-to-bill process. The IoT-enabled asset performance improvement processes can help in driving internal costs down for water companies. Using sensor technologies for monitoring real time condition of the piping infrastructure can improve the analysis of maintenance needs. The analysis of this type of sensor data can also reveal operational stress levels in different areas of the system indicating where in the infrastructure operational inefficiencies are located. The differentiating pricing models business model can help in reducing investments for extra capacity in networks with capacity problems. The water and wastewater infrastructure has limits in its capacity. When lots of people use the critical parts of infrastructure at same time, the network can become overloaded. By incentivizing the users to use water outside peak times, the load on the networks can be relieved. Similar business model is

in use already today in energy industry, where energy prices vary depending on the time of the day. Similarly, basing the pricing on peak and low hours could be utilized also in the water industry. (Cepa et al, 2016).

The smart water meters also enable completely new kind of business models, like automatic shutdown services, condition-based monitoring, water consumption monitoring for end customers, platform offering, and water consumption incentivizing. The possibility to shut down the water supply in case of leakage is one example of new business model. As the smart water meters enable real-time monitoring of the water consumption, leaks can be detected in earlier phase which can limit possible damages. The condition-based monitoring business model enables more convenient monitoring of the water pipelines. For example, individual household pipelines could be utilized with sensors and the sensors data then used for monitoring the condition of the pipelines. In the water consumption monitoring for end customers business model, a web service or mobile application could be offered for the users. The users could then use the service for monitoring water usage and optimize their water consumption. In the platform offering business model the data gathered from the water networks could be offered to third parties. The data could be used for creating new customer experiences based on the knowledge of water consumption. In the water consumption incentivizing business model, users could incentivized to use less water. The prices could be increased after certain limit is exceeded or the water supply could be turned off after certain limit. (Cepa et al, 2016).

For this case example, three different roles for the target company were identified. In the first role, the target company acts as a device retailer. In the second role, the target company acts as a retailer of the physical devices and in addition, a retailer of limited services. In the third role, the target company offers a full service offering, including the physical devices and full services related to it.

The first and the simplest role is the role, where the target company only acts as a device retailer (see fig. 4.4). The smart water meter devices would be offered by device manufacturers or white label manufacturing can be utilized. The target company either has no role at all in the provision of any services related to the offering or the role is very limited. The limited role could be a partnership with some service provider, where certain services are recommended to be bought as part of the device. The content of the service offering would be fully based on the supply of either the device manufacturers or third parties. The customers for the target company in this role would mainly be the water service companies.

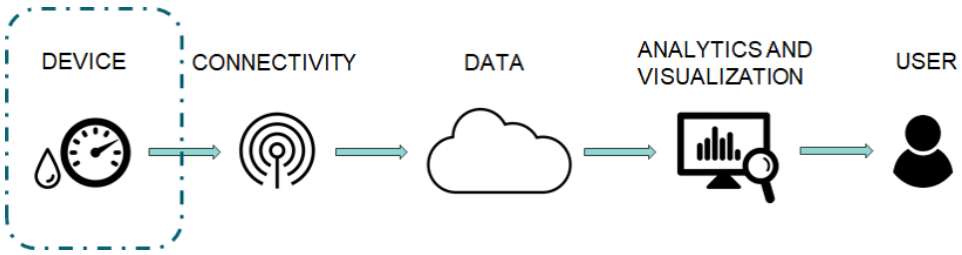

Figure 4.4: Device retailer role.

The advantage of this role is that the possible risks related to the service offerings are practically nonexistent. The target company is only responsible for matters relating to the physical product, but has no obligations or responsibilities related to the services. There are multiple technical, social, and business related risks that need to managed associated to the services. In this role, there is no need for the target company to obtain any technical capabilities, like software platforms, or organizational capabilities, like training employees to manage the new service business.

The obvious disadvantage of this role is that the target company will not be part of the digitizing smart water meter market and will not be able to benefit from the opportunities it can offer. Another disadvantage which can arise when the device manufacturers are responsible for the service offerings is that the compatibility of devices and related services can be notably reduced. As the standardization in the IoT environment is still very limited, there is a risk that the offerings will be siloed, which will cause challenges, especially for the water companies. If this happens, it will make the realization of the possible benefits of the IoT more difficult.

In the second role, the target company retails both, the physical devices, and a limited service offering (see fig. 4.5). The service offering in this role would consist of the transferring of data from device to the data storage, and offering interfaces for obtaining the data from the data storage. Analytics, enrichment of the data, nor any user interfaces are not included to the service offering. The customers for the target company in this role would mainly be the water service companies, but the data could also be offered to other parties, like housing companies.

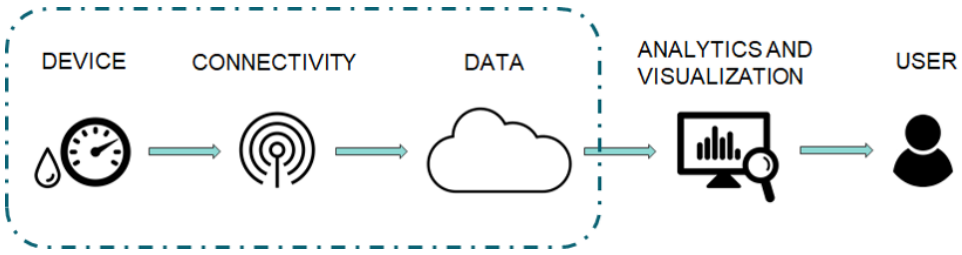

Figure 4.5: Retailer with services.

The advantages of this role are that the the target company would be a part of the digitizing smart water meter market and would able to benefit from the opportunities it can offer. The target company would also be a part of the value creation and business development of the customers. As the smart water meters are a novel business, there most probably will be numerous new business requirements forming in the future, which will offer new business possibilities. In this role, the target company would also get the possibility to get started with a new type IoT service business, which would help as the number of IoT applications grows in the future.

In this role, the target company would have to obtain some technical and organizational capabilities. The target company would be responsible - in addition to the physical devices - of the transfer and management of the data, as well as creating and managing the necessary interfaces where the data could be retrieved. Some technical capabilities, like connectivity between devices and the data storage, and a platform where the data is stored and where it can be retrieved would be needed. The technical capabilities could be done in cooperation with different partners, like network operators and IoT service providers, or they could be built using subcontractors. The risks associated to needed technical capabilities are related to the evolving IoT technologies. If the chosen and supported network protocols and technologies prove to be incorrect, it can lead to significant cost increases. This role would also need some changes to organizational capabilities. Building and maintaining the technical environment would require staff and know-how. Also, the existing sales personnel would need to be trained to offer the new services to customers.

The third role would include the retailing of the devices and full service offering (see fig. 4.6). In this role, the target company would be responsible for both, the retailing of the devices, and the full service offering. The service offering would include data transfer from the devices to data storage, storing the data, data analysis and possible enrichment with other relevant data,

and also the required web services or mobile applications for different actors. The customers for the target company in this role would be the water service companies as well as housing companies and consumer customer. This role would also make it possible to offer the services to other actors, like insurance companies and form a ecosystem around the water metering services.

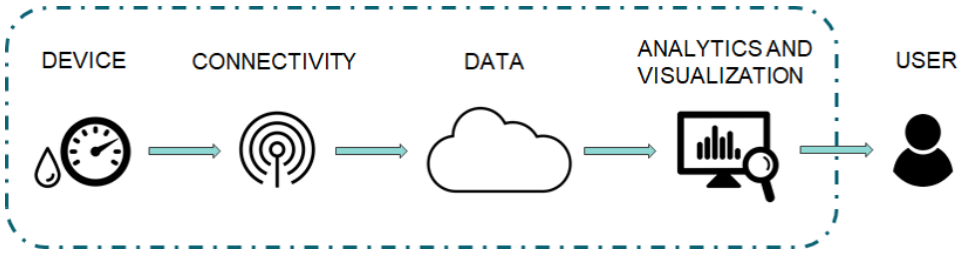

Figure 4.6: Retailer with full services.

The advantages related to this role - in addition to the benefits of the previous role - include the possibility for the target company to act as a keystone player in the forming ecosystem. This role would create the possibility to act as the facilitator of the whole for the target company. The target company could create a new layer on top of the existing individual layers, which would not be dependent of the functionalities of the physical devices, sensor setup, or network technologies. This could prevent the siloing of the service offerings, which would be beneficial for the end customers. As the siloing of the services is minimized, the full benefits of the IoT could be achieved. This role would also make it possible to expand the IoT offerings in the building and technical trade sector.

Taking this type of role would require significant investments on both, technical and organizational capabilities. The risks related to the previous role would apply also to this role. In addition, the target company would be responsible for the full service offering, including data transfer from the devices to data storage, storing the data, data analysis and possible enrichment with other relevant data, and also the required web services for different actors. Building and maintaining the technical platform would require investments on personnel and new competences would be required. The service business would need to be integrated with the sales business more tightly, which would need investments on organizational capabilities.

4.3 Discussion and conclusions of the case study

As it can be seen from the aforementioned case study, digitizing the water and wastewater industry can offer many benefits. The Finnish Ministry of Environment changed the regulation related to water and wastewater systems of buildings in 2011 to include water meters on every apartment (Ministry of Environment, 2010). However, the Finnish Government has so far not forced remotely readable water meters as it was done with electricity meters in 2009 (Finnish Government, 2009). The most recent regulation related to water and wastewater systems of buildings is from 2017 (Ministry of Environment, 2017).

Even though the usage of remotely readable water meters is not forced by regulations, it is possible that the smart metering solutions could offer benefits similar to the energy field, where the smart grid has been under active development for longer time. The IoT enabled solutions can offer many improvements to existing business models, as well as enable many completely new business models. The improvements to existing business models range from consumption based billing and possibility to create different pricing models, to better monitoring and management of the condition of the infrastructure. The completely new business models include business models, like automatic shutdown services, condition-based monitoring, water consumption monitoring for end customers, platform offering, and water consumption incentivizing.

However, it is also clear that the digitalization of water and wastewater industry also contains numerous challenges. All of the barriers of adoption presented in this thesis also apply to smart water metering. The main challenges in the smart water metering environment are related to security and privacy, data management, and financial as well as organizational challenges. As the water infrastructure is a critical asset to the society, it is important to understand and manage all security issues when applying IoT solutions. Also, it is important to consider how to manage the vast amounts of data generated by the IoT devices, and how to generate meaningful information from the data. The digitization efforts in the water and wastewater industry also needs to create some additional value to the users and at the same time needs to be economically viable. Finally, it is important to understand what kind of competence requirements the IoT enabled solutions require and what kind of effects it has to business processes.

As it can be seen from the conceptualization of the IoT business opportunities, there are many possible roles available for the target company to take.

The most simple role would be to continue business as is, retailing the devices, and leave the digitization efforts to others. The risks would stay low and the target company could stay in a monitoring position and look how the digitization of the industry evolves. This of course could also mean, that the target company could be left behind and getting involved to the new business in the future would be difficult.

Other possible roles would mean taking part to some kind of services related to smart water metering. The possible service offering could vary from very limited services to full service offering. The limited service role would include offering connectivity and data management services, and the full service role would in addition include analytics and visualization of the data. The amount of offered services would affect on the required technical and organizational capabilities. The service roles would contain risks related to the evolving technologies as well as financial aspects. The size of the role of the target company would vary from being just one actor in the ecosystem to being a keystone player, who acts as the facilitator of the whole.

Both of the service roles would include the target company to the digitizing smart water meter market and enable the target company to benefit from the opportunities it can offer. Both service roles would open up the possibility to participate to the value creation and business development of the customers. The service roles would also offer the possibility to get started with a new type of IoT service business. The business domains on which the target company operates are ones, where the IoT will most probably cause major disruption in the future. It would be beneficial for the target company to start generating knowledge of the possibilities that the IoT solutions can offer in a early phase.

Chapter 5

Conclusions

The research problems that led to the implementation of this study consisted of the difficulty to understand, what the IoT actually is, and what kind of opportunities it has to offer. At the time of this study, the target company didn't have means to create a sufficiently comprehensive understanding of the opportunities offered by the IoT. In addition, as the IoT is a complex phenomenon in terms of monetization, It was difficult for the target company to create a comprehensive understanding on where the real value of the IoT comes from. Therefore it was interesting for the target company to understand what kind of business possibilities the IoT can offer.

The goal of this study was to to create a view or a framework of possible IoT business opportunities for the target company. This was done by creating a conceptualization that unfolded the different roles there are in IoT business for the target company to take or aim for. In addition to the conceptualization, there was also a need to create better understanding of the customership and value proposition related to the IoT business, and recognize the most important barriers of adoption and capabilities required for managing the barriers of adoption.

After defining the key concepts in chapter two, the overall architecture and the technology stack of the IoT, the expanding of industry boundaries caused by the IoT, and a overview of IoT business models was first described in chapter three. After that, a literature study was done and discussions were conducted with the key personnel of the target company for recognizing the key phenomena affecting the roles the target company might want to position itself when considering commencing IoT business. Three distinct phenomena influencing the possible roles were recognized, being the servitization of manufacturing, platform economy, and ecosystems. Based on the recognized

key phenomena, a conceptualization of IoT business opportunities was presented. The conceptualization of the IoT business opportunities was created through a framework which combined the possible roles and positions for the target company to take. The framework was expressly described from the point of view of the target company.

After the framework was created, the technical, social, and business related challenges that companies and users may face when implementing and using IoT solutions, as well as needed capabilities for managing them was presented. After the literature study, the empirical study was conducted. Chapter four presented one concrete use case, smart water metering, in perspective of the created conceptualization of IoT business opportunities.

5.1 Research questions revisited

This section revisits the original research questions presented in this thesis.

Q1: What aspects should the target company consider when starting IoT business?

When considering the aspects that should be considered when planning on starting IoT business, it is important to first understand the key concepts related to the IoT. The key things to be defined are the overall architecture and the technology stack of the IoT, what effect does the expanding of industry boundaries caused by the IoT create, and to understand, what kind of business models the IoT can offer. The high-level architecture of the IoT can be presented as a 3-layered or a 5-layered architecture. The 3-layered architecture consists of perception layer, network layer, and application layer. The 5-layered architecture consists of perception layer, transportation layer, processing layer, application layer, and business layer. The IoT products create a completely new requirements for technology infrastructure for companies to build and support. The IoT technology stack consists of multiple layers, including product hardware and embedded software, connectivity, and a product cloud, which consists of a application platform and software applications running on remote servers.

The increasing capabilities of the IoT products not only affect the competition between companies within industries, but expand the industry boundaries. For the companies to able to answer the broader need of the customer, they need to widen the competitive boundaries of an industry with a set of related products. This shifts the competition from a discrete product to a

broader product system, where the company is just one actor. This, however, is not enough but the industry boundaries are expanding even beyond product systems towards systems of systems. As the IoT-enabled products become more and more commoditized, businesses are forced to find new ways to create and capture value. At the first stages, the IoT business models will most probably heavily borrow from existing business models but also novel business models start to emerge.

After these key concepts are defined, a conceptualization of possible roles and positions for a company to take can be created. The conceptualization of the IoT business opportunities is created through a framework, which combines the possible roles and positions for a company to take. Three distinct phenomena influencing the possible roles can be recognized, being the servitization of manufacturing, platform economy, and ecosystems. The first phenomenon influencing the conceptualization of IoT business opportunities is the servitization of manufacturing. The current global economy forces manufacturing companies to adapt to an ever changing business environment. Rapidly changing business environment has created trends, such as the servitization of manufacturing. Servitization refers to a tendency of a manufacturing company to expand their tangible, product-based offering with intangible services.

The second phenomenon influencing the conceptualization of IoT business opportunities is platform economy. In their core platforms are environments, either technical, like software systems or physical, like places or goods, connecting different actors that derive value from others that participate in the platform. These different actors consists of the platform owner, users, and complementary business partners, often called complementors, which all utilize and benefit from the platform's base functionality.

The third phenomenon influencing the conceptualization of IoT business opportunities is ecosystems. Many of today's digital markets require distinctive competitive strategies because the products are parts of a larger system that combines core components and form a platform made by one company, with complementary components made by variety of others. In some cases, a platform leader emerges that works with the other companies supplying complementary products and services. Together, they form a ecosystem that greatly increases the value of the platform leader and the complementaries.

Based on the aforementioned phenomena, a conceptualization of IoT business opportunities was created. The basis of the conceptualization is on manufacturing and retailing of IoT-enabled products. In manufacturing role, companies can either manufacture their own IoT-enabled products or white label

products can be used. In retail role, companies retail IoT-products manufactured by other companies. In these roles the possible services attached to the offering are not included.

The services role can be included to both, manufacturing and retailing roles. In manufacturing role the manufacturing company can create and control the services created on top of the products. In retailing role the retailer can sell a combination of products and services, act as a service provider or a facilitator and participate to the creation of the service offerings in cooperation with the manufacturing company, or create own services on top of the products and control what kind of services are offered as part of a product offerings.

As services are included into the product offering, a need for platform emerges. A third party platform can be utilized or own platform can be created for the service offerings. The platform itself can be in control of the manufacturing role, the retailer role, or in control of a third party. The owner of the platform can make the decisions on the openness of the platform. The platform can be made either internal, when only the owner has access to it, partially open, when some actors in addition to the platform owner has access to it, or open, when all actors have access to the platform. Depending on the type and role of the possible platform, a possibility of a ecosystem creation emerges. The manufacturing and retailing roles can be an actor or a central keystone actor in the ecosystem. Again similarly as mentioned before, the owner of the platform or the keystone player in the ecosystem has a major impact on how the realization of the potential of the IoT applications will happen. The platform owner can make decisions, which leads to silos, or to an more open platform. Similarly, a keystone player in a ecosystem can make decisions, which can either help or hinder the needs of other actors.

Q2: What kind of barriers of adoption are associated to the starting of IoT business and what kind of capabilities are required for managing them?

It is quite obvious, that there are numerous challenges and risks related to the IoT. Because the IoT is a novel phenomenon, businesses and individuals have to cope with many different challenges and growing pains. As the barriers of adoption and the needed capabilities for managing them were recognized for this study, three major groups for the barriers of adoption emerged. These were technical, social, and business related barriers of adoption. It is good to mention, that many of the barriers of adoption discussed in this thesis are in a way more general and apply to any other new technology as well, but there are also some unique challenges related to the IoT domain. It is also important

to point out, that the goal of this study was not to create an exhaustive list of all possible barriers of adoption, but rather to create a overview of the most critical overall aspects that will be challenging when creating IoT solutions. The barriers of adoption were also not presented in any particular order of importance and many of the challenges presented cannot be treated separately because they often contain complex interdependencies.

The technical barriers of adoption included concepts, like security, heterogeneity, trust, standardization, connectivity and interoperability, and data integrity issues, as well as challenges related to technology maturity, technical complexity, and power consumption. The overall security of the IoT is one of the main challenges related to it and the nature of the IoT solutions expose them to both, digital and physical threats. The heterogeneous nature of the IoT environments creates challenges to technical trust management. The novelty of the IoT solutions and the lack of commonly accepted standards creates challenges, especially to connectivity and interoperability. As the IoT technologies get more mature and the IoT devices become autonomous, the role of data integrity becomes more crucial and the risk on attacks against the integrity of the data increases. The technologies related to the IoT are still forming and still relatively immature, but at the same time the nature of the IoT will force the technologies to evolve very complex. Because the IoT devices will need to operate in places where continuous power supply is unavailable, there will be challenges related to the management of power consumption.

The social barriers of adoption included concepts, like lack of common understanding, privacy, trust and data ownership issues, as well as challenges related to the governance and ethics of the IoT. Creating a common understanding about the IoT will be crucial for the realisation of the full benefits that can be achieved. Challenges related to the privacy of the IoT can be seen as one of the major issues. As the privacy requirements in the IoT environments are not currently covered sufficiently, there is a need for well-defined privacy policies. Behavioral trust is another topic, that will create major challenges. The users need to able to trust, that the IoT solutions will do what they are supposed to do, without bringing harm to the user. As the IoT will present a completely new world when considering the rights and protection of individuals, completely new governance mechanisms and ethical guidelines are also needed.

The barriers of adoption related to the businesses implementing IoT solutions consists of monetization and financial challenges, long time to value, and uncertain demand of IoT solutions, as well as challenges related to competence

requirements, business processes, scalability, contractual difficulties, and operating in multi-vendor environments. As majority of the IoT solutions will require significant investments and long periods of time for development, there will be difficulties in the monetization of the IoT. Also it seems to be somewhat unclear, how the IoT is going to improve the financial results of businesses. As many of today's IT projects, also IoT projects can take a long time. In addition, it seems that the demand for IoT solutions in consumer and business sides varies significantly. In the future, the IoT will create a need for completely new skills, and when consumers become producers, there will be a need for new generation of digital experts capable of understanding both the new technologies and also the societal impacts of widespread adoption of these technologies. There are many differences when comparing IoT services to common enterprise services. Technical implementation, communication model, and and the orchestration of services can be different which can cause challenges to existing business processes. Companies can also run into problems when they start to expand their IoT projects over time. Many aspects that are valid for the contracts in the ICT environment will be equally valid to the majority of IoT contracts, so the same challenges will also apply. Finally, todays IoT solutions almost never come from one individual vendor which can cause challenges in vendor management.

5.2 Implications and limitations

Even though the topic of IoT is being studied more and more, there are still many areas that are quite narrowly researched and more research is needed. Studies related to the barriers of adoption related to the IoT are already quite extensive. The conceptualization of IoT business opportunities presented in this thesis, while created solely to the use of one retailer company, can be utilized in other businesses as well.

It is quite certain, that the amount of IoT solutions will greatly increase in the future and it can be difficult to create sufficient understanding on who a company should position itself. As it can be seen from the case study, using this kind of framework can clarify the possibilities and needed capabilities, especially in the early stages, when examining some IoT use case.

As mentioned earlier, the conceptualization presented in this thesis is done purely in perspective of one company. For that reason the findings in this thesis cannot necessarily be used in other industries and not even in other businesses in the building and technical trade. Another limitation comes

from the number of employees of the target company with whom the discussions related to the framework were held. There were only few persons who evaluated the framework during the study and they were all from the target company's building and technical trade.

5.3 Possible future works

As the conceptualization of IoT business opportunities created in this thesis was only tested with one use case, it could be interesting to use it in other use cases, perhaps even in the other sectors of the target company, being the retail trade and car trade. In addition, it would be interesting to use the conceptualization in some other company's use cases, like for example in a manufacturing company.

As mentioned in the beginning of this thesis, there are numerous different phenomena presently happening, that are part of the digitalization of businesses. It would also be interesting to study, how these other phenomena, like artificial intelligence, machine learning, and blockchain affect to the development of the IoT.

Appendix A

IoT innovation workshops

As a part of this thesis, two IoT innovation workshops were organized. The goal of the workshops was to create understanding on customership and value proposition of the IoT. The target of the first workshop was to create understanding on a general level and in perspective of the target company, who are the customers, what kind of different actors and roles there are in the IoT business, and where does the value come from. The target of the second workshop was to innovate some IoT products or services for the target company to start with.

The first workshop focused on studying the IoT environment in perspective of the conceptualization of IoT business opportunities and through the different roles presented in the conceptualization: retail, manufacturing, platform and ecosystem. Firstly, the customers in the IoT business environment were identified. Secondly, other actors and possible roles were identified. Thirdly, the value generation to different stakeholders were identified.

The second workshop focused to innovate different IoT products and services for the target company's building and technical trade sector. Four different application domains were selected for creating the IoT products and services. The application domains were connected living and working, smart retail and supply-chain, connected health, and smart energy. All of the application domains were studied in perspective of both, business to customer, and business to business customership.

A.1 First workshop

In the first workshop, the possible customers in the IoT business environment based on the roles were first identified. Also other actors and possible roles

were identified. Finally, the value generation to different stakeholders were discussed. In the retailer role, the identified customers included consumer customers, construction companies, maintenance companies, housing companies, installation service providers, manufacturing industry, other retailers, municipalities and cities, public sector, and also startup companies. Other actors and possible roles in the retailer role that were identified, included application developers, security companies, insurance companies, healthcare sector, and legal service providers. The value generation discussion on retailing focused on the role of data brokers, the issues related to device monitoring, remote control, and maintenance services. Also, the effect the IoT devices may have to insurance premiums were discussed.

In the manufacturer role, the identified customers included designers, contractors, service companies, consumer customers, public sector customers, and infrastructure network operators. Other actors and possible roles in the manufacturer role were real estate companies, industrial plants and factories, installation companies, third party data sources and application providers, cloud operators, and product designers. The value generation discussion on manufacturing focused on issues related to the ownership of data, and how the data could be efficiently targeted to relevant parties.

In the platform role, the identified customers included stores, logistics including warehouse operations and transport companies, manufacturers and suppliers, public facilities, and building contractors. Other actors and possible roles in the platform role were the possible owners and operators of the platform, and third parties, like insurance companies. The challenges related to the platform role included issues related to who builds and operates the possible platform, how will the revenue generation be organized in this kind of platform environment, how will the partner network be created and committed to the platform, how will the broad knowledge requirements be fulfilled, and how will the scalability of the platform be ensured. The value generation discussion on platform role focused on issues like who is responsible of the development of the platform, who owns the data and who has access to the data and on what basis, how will the marketing of the platform be organized, and how will the data processing and refinement be organized.

In the ecosystem role the identified customers, other actors and different role were very similar as in the platform role. In addition, B2C and B2B customers, partners, different service providers, and startup companies were identified. The value generation discussion on ecosystem role focused on who will be the facilitator of the ecosystem, how will the value network form, how

will the communication and transactions between actors be organized, how will the need for continuous development of the ecosystem be fulfilled, and how will the use of different kinds of data be handled.

Also, a small innovation session was organized in the first workshop. The goal was to innovate different kinds of IoT products and services that would be further developed in the second workshop. The groups were able to create over 300 different IoT related products and services during the workshop. Four different ideas from four different application domains were selected to be further developed in the second workshop.

A.2 Second workshop

In the second workshop, four different application domains were selected for more detailed service design. The application domains were connected living and working, smart retail and supply-chain, connected health, and smart energy. Connected living and working focused on a service platform for consumers to bring together living related data and products. Smart retail and supply-chain focused on utilization of RFID in supply-chain management. Connected health focused on a service platform for consumers, that brings together health and nutrition. Smart energy focused on building specific optimization of energy consumption.

Connected living and working: service platform for consumers that brings together living related data and products. The customers in service platform for consumers that brings together living related data and products include consumer customers, project customers, renovation companies, and constructors. The consumer customers and project customers are typically families or couples. They value security, easiness, and possibility for cost savings. Their common objections include continuity of IoT solutions, hacking risks, and risks related to safety. Their change expectations and purchase criteria is based on the continuity of the solutions, trust towards the vendor, cost, and information security. The consumer customers can be reached in physical stores and web. The renovation companies are typically small or midsized companies. They value traditional and familiar solutions. Their common objections include risk of not being able to answer new customer needs and losing money and customers. Their change expectations and purchase criteria is based on reliable and easy to install solutions, available training, price, and partners. The renovation companies can be reached via B2B sales channels. The constructors are typically larger companies. They value higher

profits. Their common objections include solution maturity and maintaining customer relationships. Their change expectations and purchase criteria is based on partnership, quality, costs, and reliability. The constructors can be reached via B2B sales channels.

The crucial problems, that the customers face in the service platform for consumers that brings together living related data and products are related to safe living, cost savings, and the diversity of available solutions. Safe living includes things, like air quality, humidity measurements, and fire safety. Cost savings include things, like water consumption and electricity consumption. Diversity of available solutions includes things, like compatibility challenges, difficulties in installation, and information and data security challenges. The unique value proposition is the possibility to offer widest selection of solutions. The defining element of the solution is a platform offered by global actor and who has reliable distribution channels, products, and partners. The interaction with customers happens in stores and via web. The advantage for the target company comes from hundreds of physical stores and data.

Smart retail and supply-chain: utilization of RFID in supply-chain management. The customers in the utilization of RFID in supply-chain management include consumer customers, contractors, and project customers. The consumer customers are typically families or couples. They value staying in budget. Their common objections include cost overruns, dealing with other actors, and detailed planning. Their change expectations and purchase criteria is based on trustworthiness, vision, quality, and price. The consumer customers can be reached in physical stores and web. The contractors are typically project managers in construction sites. They value finishing projects on time and in budget. Their common objection is failure in delivery. Their change expectations and purchase criteria is based on prompt deliveries and flexibility of planning. The project managers as a customers can be reached in the construction site or via phone or email.

The crucial problems, that the customers face in the utilization of RFID in supply-chain management includes too time consuming shopping in stores and the lack of real time transportation status and delivery information. The unique value proposition is the possibility to offer reliable customer experience and delivery of products. The defining elements of the solution are RFID tags for products and mobile application for the customers. The RFID tags enables product identification throughout the lifecycle of the product, can trigger auto replenishment, and can trigger notification to the customers. The mobile application enables the displaying of customers information, payment information, product search, navigation in store, tracking of deliveries,

and communication with sales personnel. The interaction with customers happens in stores and via web. The advantage for the target company comes from best omnichannel customer experience.

Connected health: service platform for consumers, that brings together health and nutrition. The customers in service platform for consumers, that brings together health and nutrition consists mainly of consumer customers. The consumer customers can be people who are interested in health and nutrition and elderly persons and their relatives. The people who are interested in health and nutrition are typically technological forerunners and they have deep interest in health and nutrition. The value improvement on quality of life. Their change expectations and purchase criteria is based on new innovations and trends. They can be reached via web. The elderly person's value health and meaningful life. Their change expectations and purchase criteria is based on preventative healthcare, safety, and health monitoring. They can be reached in physical stores.

The crucial problems, that the customers face in the service platform for consumers, that brings together health and nutrition are how to recognize one's own health and how reliable the partner, who manages the health related data is. The unique value proposition is the possibility to offer reliable service and localized services. The defining elements of the solution are a secure solution that has simple, clear, and easy to use user interfaces. The interaction with customers happens in physical stores and web and through partner network. The advantage for the target company comes from existing data, financial status, and from being a established and reliable actor.

Smart energy: building specific optimization of energy consumption. The customers in building specific optimization of energy consumption include homeowners, real estate maintenance and management, and local energy providers and distributors. The homeowners are typically middle class families, who reside in larger cities or suburbs. They value environment and sustainability and appreciate free time. Their common objections are changes in energy prices and prejudice towards new technologies. Their change expectations and purchase criteria is based on energy and cost savings, return on investment, standard of living, comfortability improvements, and ease of use. The homeowners as a customers can be reached in the stores and web. The real estate maintenance and management are typically commercial companies who are either owners of the buildings, or service providers. They value business approach, profit optimization, and social responsibility. Their common objections are related to new technologies, where references

are usually needed, and technology relevance to the business domain. Their change expectations and purchase criteria is based on return on investment and uninterrupted processes. The real estate maintenance and management as a customers can be reached via B2B sales channels.

The crucial problems, that the customers face in the building specific optimization of energy consumption include difficulties to understand and determine, how the energy is consumed, difficulties to monitor and control the usage of energy, especially in industrial spaces, and imbalance between energy surplus and demand. The unique value proposition is the possibility to offer complete solution and full service offering related to it. The defining elements of the solution are intelligent control, platform for connecting devices, wide availability, modular and scalable solution that integrates all sources, that consume energy. The interaction with customers, both B2C and B2B, is omnichannel. The advantage for the target company comes from scale and reach, distribution channels, and vast data assets.

A.3 Conclusions

The workshops proved to be quite useful for creating understanding on IoT in perspective of the target company. Identification of the customers, other actors, and roles seemed to be an easier task and the groups were able to study these aspects quite thoroughly. A large variety of customers and customer's customers were identified. Also different possible roles for the target company were quite widely recognized. The concept of value was a more difficult topic. It was known already before the workshops, that the IoT is a complex phenomenon in terms of value and monetization. For example, the discussions related to the creation of value networks beyond traditional value chains remained quite light and would require more studying.

References

1. Abdmeziem, M. R., Tandjaoui, D., and Romdhani, I. (2016), Architecting the internet of things: state of the art, In Robots and Sensor Clouds, pp. 55-75, Springer International Publishing.

2. Algaze, B. (2016) Building Software Products vs Platforms, [Online], Available: https://blog.frogslayer.com/building-software-products-vs-platforms/ [Accessed: 27 January 2018].

3. Almeida, V., Doneda, D. and Monteiro, M. (2015) Governance challenges for the Internet of Things, IEEE Internet Computing 19.4 (2015), pp. 56-59.

4. Amaratunga, D., Baldry, D., Sarshar, M., and Newton, R. (2002) Quantitative and qualitative research in the built environment: application of "mixed" research approach, Work study, 51(1), pp. 17-31.

5. Ashton, K. (2009) That "internet of things" thing, RFID journal, 22(7), pp. 97-114.

6. Avlonitis, V., Frandsen, T., Hsuan, J., and Karlsson, C. (2014) Driving competitiveness through servitization: A guide for practitioners.

7. Baines, T. S., Lightfoot, H. W., Benedettini, O., and Kay, J. M. (2009) The servitization of manufacturing: A review of literature and reflection on future challenges, Journal of Manufacturing Technology Management, 20(5), pp. 547-567.

8. Baldini, G., Botterman, M., Neisse, R. and Tallacchini, M. (2016) Ethical design in the internet of things, Science and engineering ethics (2016), pp. 1-21.

9. Bannan, C. (2016) The IoT threat to privacy, [Online], Available: https://techcrunch.com/2016/08/14/the-iot-threat-to-privacy/ [Accessed: 2 June 2017].

10. Benson, M. (2017) Building An Organizational IoT Competency: What You Need To Know [Online], Available: https://www.forbes.com/sites/forbestechcouncil/2017/04/21/building-an-organizational-iot-competency-what-you-need-to-know/#7a7ab7c63cf7 [Accessed: 30 September 2017].

11. Best, J. (2016) Who really owns your Internet of Things data?, [Online], Available: http://www.zdnet.com/article/who-really-owns-your-internet-of-things-data/ [Accessed: 16 March 2017].

12. Blaauw, D., Sylvester, D., Dutta, P., Lee, Y., Lee, I., Bang, S., Kim, Y., Kim, G., Pannuto, P., Kuo, Y.S., Yoon, D., Jung, W., Foo, Z., Chen, Y.P., Oh, S., Jeong, S. and Choi, M. (2014) IoT design space challenges: Circuits and systems, In VLSI Technology (VLSI-Technology): Digest of Technical Papers, 2014 Symposium on (pp. 1-2), IEEE.

13. Boley, H., and Chang, E. (2007) Digital ecosystems: Principles and semantics, In Digital EcoSystems and Technologies Conference, 2007, DEST'07, Inaugural IEEE-IES, pp. 398-403, IEEE.

14. Boos, D., Guenter, H., Grote, G., and Kinder, K. (2013) Controllable accountabilities: the internet of things and its challenges for organisations, Behaviour & Information Technology, 32(5), pp. 449-467.

15. Briscoe, G., and De Wilde, P. (2006) Digital ecosystems: evolving service-orientated architectures, In Proceedings of the 1st international conference on Bio inspired models of network, information and computing systems, ACM.

16. Brynjolfsson, E. and McAfee, A. (2016) The Second Machine Age, New York: W. W. Norton.

17. Bucherer, E., and Uckelmann, D. (2011) Business models for the internet of things, Architecting the internet of things, pp. 253-277.

18. Bui, T. (2016) The Internet of Things: What the hell is an "IoT platform"?, [Online], Available: https://www.itproportal.com/2016/08/01/the-internet-of-things-what-the-hell-is-an-iot-platform/ [Accessed: 24 February 2018].

19. Burrus, D. (2014) The Internet of Things Is Far Bigger Than Anyone Realizes, [Online], Available: https://www.wired.com/insights/2014/11/the-internet-of-things-bigger/ [Accessed: 25 November 2017].

20. Butler, B. (2018) What is fog computing? Connecting the cloud to things, [Online], Available: https:// www. networkworld. com/ article/ 3243111/ internet-of- things/ what-is-fog- computing- connecting-the-cloud- to-things.html [Accessed: 27 July, 2018].

21. Buyya, R. and Dastjerdi, A.V. (2016) Internet of Things: Principles and paradigms, Elsevier.

22. Cannon, H., Feinstein, A. and Friesen, D. (2014) Managing complexity: applying the conscious-competence model to experiential learning, Developments in Business Simulation and Experiential Learning 37 (2014).

23. Cepa, K., Chen, H.H., Laakso, T., and Nelimarkka, M. (2016) Disrupting the Water Industry, Digitalization, 203.

24. Chase, J. (2016) Where, really, is the ROI in IoT?, [Online], Available: http://dataconomy.com/2016/07/where-really-is-the-roi-in-iot/ [Accessed: 24 September, 2017].

25. Chen, E.T. (2017) The Internet of Things: Opportunities, Issues, and Challenges, In The Internet of Things in the Modern Business Environment, pp. 167-187, IGI Global.

26. Chen, S., Xu, H., Liu, D., Hu, B., and Wang, H. (2014) A vision of IoT: Applications, challenges, and opportunities with china perspective, IEEE Internet of Things journal, 1(4), pp. 349-359.

27. Chen, Y.K. (2012) Challenges and opportunities of internet of things, In Design Automation Conference (ASP-DAC), 2012 17th Asia and South Pacific, pp. 383-388), IEEE.

28. Chesbrough, H. (2010) Business model innovation: opportunities and barriers, Long range planning, 43(2), pp. 354-363.

29. Christensson, P. (2015) Internet of Things Definition, [Online], Available: https://techterms.com/definition/internet_of_things [Accessed: 28 July, 2018].

30. Church, Z. (2017) Platform Strategy, Explained, [Online], Available: http://mitsloan.mit.edu/newsroom/articles/platform-strategy-explained/ [Accessed: 22 January 2018]

31. Cisco. (2013) The Internet of Everything and the Connected Athlete: This Changes Everything, [Online], Available: https:// www.cisco.com /c/en/us/ solutions/ collateral/ service-provider/ mobile-internet/ white_ paper_ c11-711705.html [Accessed: 7 August 2018].

32. Clements, M. T. (2004) Direct and indirect network effects: are they equivalent?, International Journal of Industrial Organization, 22(5), pp. 633-645.

33. Columbus, L. (2017) 2017 Roundup Of Internet Of Things Forecasts, [Online], Available: https://www.forbes.com/sites/louiscolumbus/2017/12/10/2017-roundup-of-internet-of-things-forecasts/#64c710df1480 [Accessed: 7 August 2018].

34. Court of Justice of the European Union. (2015) The Court of Justice declares that the Commission's US Safe Harbour Decision is invalid, [Online], Available: http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf [Accessed: 19 March 2017].

35. Court of Justice of the European Union. (2016) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC,[Online], Available: http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32016R0679&qid=1489906948864 [Accessed: 19 March 2017].

36. Cranford, N. (2017) How to build organizational IoT competence, [Online], Available: https://enterpriseiotinsights.com/20170629/how-to-build-organizational-iot-competence-tag27 [Accessed: 30 September 2017].

37. Elvy, S. (2016) Contracting in the Age of the Internet of Things: Article 2 of the UCC and Beyond, Hofstra Law Review: Vol. 44 : Iss. 3 , Article 10, Available: http://scholarlycommons.law.hofstra.edu/hlr/vol44/iss3/10

38. European Commission. (2013) Report on the Public Consultation on IoT Governance, [Online], Available: http://ec.europa.eu/ information_society/newsroom/cf/dae/document.cfm?doc_id=1746 [Accessed: 30 June 2017].

39. European Research Cluster on the Internet of Things. (2015) IoT Governance, Privacy and Security Issues, Internet of Things, [Online] European Commission, Available: http://www.internet- of-things-research.eu/

pdf/IERC_Position_Paper_IoT _Governance_Privacy_Security _Final.pdf [Accessed 2 July 2017].

40. Fabode, S. (2016) New Business Models For IoT and IIoT Businesses, [Online], Available: https://medium.com/startup-grind/new-business-models-for-iot-and-iiot-businesses-2e5177d11a4a [Accessed: 3 December 2017].

41. Faggella, D. (2017) What is Machine Learning?, [Online], Available: https://www.techemergence.com/what-is-machine-learning/ [Accessed: 27 July, 2018].

42. Farrell, J., and Klemperer, P. (2007) Coordination and lock-in: Competition with switching costs and network effects, Handbook of industrial organization, 3, pp. 1967-2072.

43. Farrell, L. (2017) Toward an ethics of the Internet of Things, [Online], Available: https://sciencenode.org/feature/toward-an-ethics-of-the-internet-of-things.php [Accessed: 4 July 2017].

44. Fearn, N. (2017) Why we need a less fragmented IoT ecosystem, [Online], Available: http://www.itpro.co.uk/mobile/28106/why-we-need-a-less-fragmented-iot-ecosystem [Accessed: 12 May 2018].

45. Finnish Government (2009) Valtioneuvoston asetus sähköntoimitusten selvityksestä ja mittauksesta, Finnish Government: Helsinki.

46. Fleisch, E., Weinberger, M., and Wortmann, F. (2015) Business models and the internet of things, In Interoperability and Open-Source Solutions for the Internet of Things, pp. 6-10, Springer, Cham.

47. Forbes Insights (2017) 4 Ways To Overcome The Complexity Of IoT Implementation, [Online], Available: https://www.forbes.com/ sites/ insights-hitachi/ 2017/12/18/4-ways-to- overcome-the- complexity-of-iot- implementation/#47e70f4b7034 [Accessed: 11 May 2018].

48. Gaillard, J.C. (2016) Internet Of Things: Data Integrity - Not Confidentiality - Is Paramount, [Online], Available: https:// channels. theinnovationenterprise .com/articles/internet-of-things-data- integrity-not-confidentiality-is-paramount [Accessed: 12 May 2018].

49. Galletto, M. (2018) A Definition of Data Mining, [Online], Available: https://www.ngdata.com/what-is-data-mining/ [Accessed: 27 July 2018].

50. Gartner. (2018a) IT Glossary, [Online], Available: https://www. gartner.com/ it-glossary/?s=digitization [Accessed: 27 July 2018].

51. Gartner. (2018b) IT Glossary, [Online], Available: https://www. gartner.com/ it-glossary/digitalization [Accessed: 27 July 2018].

52. Gassmann, O., Frankenberger, K., and Csik, M. (2013) The St. Gallen business model navigator.

53. Gates, M. (2017) IoT Glossary: 55 Terms You Need to Know, [Online], Available: https://dzone.com/articles/iot-glossary-terms-you-need-to-know [Accessed: 27 July 2018].

54. Gawer, A. (2014) Bridging differing perspectives on technological platforms: Toward an integrative framework, Research Policy, 43(7), pp. 1239-1249.

55. Gawer, A., and Cusumano, M. A. (2008) How companies become platform leaders, MIT Sloan management review, 49(2), 28.

56. Gonzales, J.A. (2018) 5 Challenges in Supporting IOT Devices, [Online], Available: https://infolink-exp.com/challenges-in-supporting-iot-devices/ [Accessed: 12 May 2018].

57. Guinard, D. (2015) Internet of things: businesses must overcome data and privacy hurdles, [Online], Available: https://www. theguardian.com/ media-network/2015/jun/01/ internet-of-things-businesses-data-privacy [Accessed 18 March 2017].

58. Hackbarth, K (2016) The three challenges of IoT solution development, [Online], Available: https://blog.bosch-si.com/internetofthings/the-three-challenges-of-iot-solution-development/ [Accessed: 12 Mayy 2018].

59. Hagiu, A. (2013) Strategic Decisions for Multisided Platforms, [Online], Available: https://sloanreview.mit.edu/article/strategic-decisions-for-multisided-platforms/ [Accessed: 18 February 2018].

60. Hagiu, A., and Rothman, S. (2016) Network effects aren't enough, Harvard business review, 94(4), 17.

61. Hagiu, A., and Wright, J. (2015) Multi-sided platforms, International Journal of Industrial Organization, 43, pp. 162-174.

62. Haller, S. and Magerkurth, C. (2011) The real-time enterprise: Iot-enabled business processes, IETF IAB Workshop on Interconnecting Smart Objects with the Internet.

63. Hayes, J. (2016) IoT Platforms: Making Sense Of It All, [Online], Available: http://www.landmobile.co.uk/indepth/iot-platforms-making-sense-of-it-all/ [Accessed: 24 February 2018].

64. Hermann, M., Pentek, T., and Otto, B. (2016) Design principles for industrie 4.0 scenarios, In System Sciences (HICSS), 2016 49th Hawaii International Conference on, pp. 3928-3937, IEEE.

65. Hossain, M.M., Fotouhi, M., and Hasan, R. (2015) Towards an analysis of security issues, challenges, and open problems in the internet of things, In Services (SERVICES), 2015 IEEE World Congress on (pp. 21-28), IEEE.

66. Hung, M. (2017) Leading the IoT, [Online], Available: https://www.gartner.com/imagesrv/books/iot/ iotEbook_digital.pdf [Accessed: 7 August 2018].

67. IBM. (2018) The internet of things: seven deadly sins of strategy and design, [Online], Available: https://www.ibm.com/internet-of-things/learn/iot-strategy-and-design/ [Accessed: 7 August 2018].

68. Klubnikin, A. (2016) Internet of Things: How Much Does it Cost to Build IoT Solution? [Online], Available: http://r-stylelab.com/company/blog/iot/internet-of-things-how-much-does-it-cost-to- build-iot-solution [Accessed: 24 September 2017].

69. Korpela, K., Kuusiholma, U., Taipale, O., and Hallikas, J. (2013) A framework for exploring digital business ecosystems, In System Sciences (HICSS), 2013 46th Hawaii International Conference, IEEE, pp. 3838-3847.

70. Kortuem, G., Bandara, A., Smith, N., Richards, M. and Petre, M. (2013) Educating the Internet-of-Things generation, Computer, 46(2) pp. 53-61.

71. Kumar, J.S. and Dhiren, R.P. (2014). A survey on internet of things: Security and privacy issues, International Journal of Computer Applications, vol. 90 - No 11, March 2014, pp.20-26.

72. Køien, G.M. (2011) Reflections on trust in devices: an informal survey of human trust in an Internet-of-Things context, Wireless Personal Communications 61.3 (2011), pp.495-510.

73. Lee, J (2016) Overcoming the three most common challenges to IoT adoption, [Online], Available: https:// blogs.microsoft.com/iot/2016/07/19/overcoming-the-three-most- common-challenges-to-iot- adoption/ [Accessed: 7 October 2017].

74. Lee, J., Bagheri, B., and Kao, H.A. (2015). A cyber-physical systems architecture for industry 4.0-based manufacturing systems, Manufacturing Letters, 3, pp. 18-23.

75. Leister, W. and Schulz, T. (2012) Ideas for a Trust Indicator in the Internet of Things, SMART, Vol. 12, 2012, pp. 31-34.

76. Liebowitz, S. J., and Margolis, S. E. (1995) Are network externalities a new source of market failure?, Research in Law and Economics, 17(0), pp. 1-22.

77. Light, R. (2016) The Internet of Things Presents Concerns over Data Ownership, [Online], Available: https:// www.g2crowd. com/blog/ internet-of-things- management/ iot-data- ownership-concerns/ [Accessed: 18 March 2017].

78. Lusch, R. F., Vargo, S. L., and O'Brien, M. (2007) Competing through service: Insights from service-dominant logic, Journal of retailing, 83(1), pp. 5-18.

79. Mahmoud, R., Yousuf, T., Aloul, F., and Zualkernan, I. (2015), Internet of things (IoT) security: Current status, challenges and prospective measures, In Internet Technology and Secured Transactions (ICITST), 2015 10th International Conference for (pp. 336-341), IEEE.

80. Manyika, J., Chui, M., Bisson, P., Woetzel, J., Dobbs, R., Bughin, J. and Aharon D. (2015) Unlocking the potential of the Internet of Things, [Online], Available: https://www. mckinsey.com/ business-functions/ digital-mckinsey/ our-insights/ the-internet-of-things- the-value-of -digitizing-the-physical-world [Accessed: 7 August 2018].

81. Marr, B. (2016) What Everyone Must Know About Industry 4.0, [Online], Available: https://www.forbes. com/sites/ bernardmarr/ 2016/06/20/what- everyone-must- know-about- industry-4-0/#1829e613795f [Accessed: 28 July, 2018].

82. Marr, B. (2018) The Key Definitions Of Artificial Intelligence (AI) That Explain Its Importance, [Online], Available: https:// www.forbes. com/ sites/bernardmarr/ 2018/02/ 14/ the-key-definitions- of-artificial-intelligence-ai-that- explain-its- importance/#1c1659ab4f5d [Accessed: 27 July, 2018].

83. Mashhadi, A., Kawsar, M. and Acer, U.G. (2014) Human data interaction in IoT: The ownership aspect, In Internet of Things (WF-IoT), 2014 IEEE World Forum, pp. 159-162.

84. Matteson, S (2017) How to calculate TCO and ROI for enterprise IoT implementations, [Online], Available: http://www.zdnet.com/article/how-to-calculate-tco-and-roi-for-enterprise-iot-implementations/ [Accessed: 23 September 2017].

85. Mazhelis, O., Luoma, E., and Warma, H. (2012) Defining an internet-of-things ecosystem, In Internet of Things, Smart Spaces, and Next Generation Networking, pp. 1-14, Springer, Berlin, Heidelberg.

86. McClelland, C. (2017) What is an IoT Platform?, [Online], Available: https://www.iotforall.com/what-is-an-iot-platform/ [Accessed: 24 February 2018].

87. Meola, A. (2018) What is the Internet of Things (IoT)? Meaning & Definition, [Online], Available: https://www.businessinsider.com/internet-of-things-definition?r=US&IR=T&IR=T [Accessed: 10 August 2018].

88. Miller, P. (2018) What is edge computing?, [Online], Available: https:// www. theverge.com/circuitbreaker/ 2018/5/7/17327584/ edge-computing-cloud- google-microsoft-apple- amazon [Accessed: 27 July, 2018].

89. Ministry of Environment (2010) Ympäristöministeriön asetus kiinteistöjen vesi- ja viemärilaitteistoista annetun ympäristöministeriön asetuksen muuttamisesta, Ministry of Environment: Helsinki.

90. Ministry of Environment (2017) Ympäristöministeriön asetus rakennusten vesi- ja viemärilaitteistoista, Ministry of Environment: Helsinki.

91. Moore, J. F. (1996) The death of competition: leadership and strategy in the age of business ecosystems, New York: HarperBusiness.

92. Nachira, F., Dini, P., and Nicolai, A. (2007), A network of digital business ecosystems for Europe: roots, processes and perspectives, European Commission, Bruxelles, Introductory Paper.

93. Namiot, D., Sneps-Sneppe, M., and Daradkeh, Y. (2017) On Internet of Things Education, In Proceedings of the 20th Conference of Open Innovations Association FRUCT, LETI University, St. Petersburg, Russia.

94. Noto La Diega, G. and Walden I. (2016) Contracting for the "Internet of Things": looking into the Nest, in European Journal of Law and Technology, Vol 7, No 2, 2016.

95. Novison, M. (2016) Industry Experts: Culture, Complexity Biggest Barriers To Adopting IoT In Agriculture [Online], Available: http:// www.crn.com/ news/networking/ 300081595/industry-experts- culture-complexity- biggest-barriers- to-adopting-iot-in- agriculture.htm?itc= refresh [Accessed: 7 October 2017].

96. O'Donnell, B. (2015a) The Analytics of IoT, [Online], Available: https:// techpinions.com/ the-analytics-of-iot/ 40962 [Accessed: 19 September 2017].

97. O'Donnell, B. (2015b) The IoT Monetization Problem, [Online], Available: https://www.recode.net/2015/8/5/11615348/the-iot-monetization-problem [Accessed: 19 September 2017].

98. O'Kelley, B (2017) Product And Platform, [Online], Available: https:// www. forbes.com/ sites/ ciocentral/ 2017/03/ 22/product- and- platform/ #231abe0a7c6e [Accessed: 27 January 2018].

99. Oettinger, G. (2016) Speech at the Conference "Building European Data Economy", [Transcript], Available: https:// ec.europa.eu/ commission/ commissioners/ 2014-2019/ oettinger/ announcements/ speech-conference-building- european-data- economy_en [Accessed: 11 March 2017].

100. Osterwalder, A., and Pigneur, Y. (2010) Business model generation: a handbook for visionaries, game changers, and challengers, John Wiley & Sons.

101. Oxford Dictionary. (2017) Definition of ethics in English, [Online], Available: https://en.oxforddictionaries.com/definition/ethics [Accessed: 4 July 2017].

102. Paiola, M. (2017) Digital servitization: opportunities and challenges for Italian SMES.

103. Partanen, K. (2013) Hukkaputket, [Online], Available: http:// omakotile-hdet.fi/ hukkaputket/ [Accessed: 8 June 2018].

104. Paschou, T., Adrodegari, F., Perona, M., and Saccani, N. (2017) The digital servitization of manufacturing: a literature review and research agenda.

105. Porter, M. E., and Heppelmann, J. E. (2014) How smart, connected products are transforming competition, Harvard Business Review, 92(11), pp. 64-88.

106. Press, G. (2014) 12 Big Data Definitions: What's Yours?, [Online], Available: https://www.forbes.com/sites/gilpress/2014/09/03/12-big-data-definitions-whats-yours/#c7ed64713ae8 [Accessed: 27 July, 2018].

107. Rebbeck, T. (2017) Barriers to IoT adoption: Removing inhibitors may create new opportunities [Online], Available: https:// internetofbusiness.com/ barriers-iot-adoption- opportunities/ [Accessed: 7 October 2017].

108. Riahi, A., Challal, Y., Natalizio, E., Chtourou, Z., and Bouabdallah, A. (2013) A systemic approach for IoT security, In Distributed Computing in Sensor Systems (DCOSS), 2013 IEEE International Conference on (pp. 351-355), IEEE.

109. Rodriguez, S. and Stammati, L. (2018) The Economic Impact of IoT, [Online], Available: https:// www. frontier- economics. com/ documents/ 2018/03/ internet-things _march-2018.pdf [Accessed: 11 August 2018].

110. Rouse, M. (2014) Internet of Things privacy (IoT privacy), [Online], Available: http:// internetofthingsagenda. techtarget. com/ definition/ Internet-of- Things- privacy-IoT- privacy [Accessed: 2 June 2017].

111. Rouse, M. (2015) IoT security (Internet of Things security), [Online], Available: http://internetofthingsagenda.techtarget.com/definition/IoT-security-Internet-of-Things-security [Accessed: 6 August 2017].

112. Rymaszewska, A., Helo, P., and Gunasekaran, A. (2017) IoT powered servitization of manufacturing - an exploratory case study, International Journal of Production Economics.

113. Sicari, S., Rizzardi, A., Grieco, L.A. and Coen-Porisini, A. (2015) Security, privacy and trust in Internet of Things: The road ahead, Computer Networks 76 (2015), pp.146-164.

114. Silverstein, K. (2017) The Internet of Things Will be Bigger Than the Internet Itself, Expert Says, [online], Available: https:// www. environmentalleader. com/2017/ 06/internet- things- will- bigger- internet- expert- says/ [Accessed: 25 November 2017].

115. Sookne, K. (2016) Connecting Legacy Systems to the Internet of Things, [Online], Available: https://www. automationworld. com/ article/ technologies/ networking- connectivity/ connecting- legacy- systems- internet- things [Accessed: 11 May 2018].

116. Stackpole, B. (2015) Four Skills You'll Need to Add in the Internet of Things Age, [Online], Available: https://www.ptc.com/en/cad-software-blog/four-skills-youll-need-to-add-in-the-internet-of-things-age [Accessed: 30 September 2017].

117. Suarez, F. F., and Kirtley, J. (2012) Dethroning an established platform, MIT Sloan Management Review, 53(4), 35.

118. Talbot, A. (2016) Privacy Laws: How the US, EU and others protect IoT data (or don't), [Online], Available: http://www. zdnet.com/article/ privacy-laws-how- the-us-eu-and- others-protect-iot- data-or-dont/ [Accessed 19 March 2017].

119. Techopedia. (2017) Computer Ethics, [Online], Available: https:// www.techopedia. com/definition/ 5499/computer- ethics [Accessed: 4 July 2017].

120. Techopedia. (2018) Cloud Computing, [Online], Available: https://www. techopedia. com/definition/ 2/ cloud- computing [Accessed: 27 July, 2018].

121. The European Commission. (2016) Commission Staff Working Document: Advancing the Internet of Things in Europe, Accompanying the Document Communication from the Commission to the European Parliament, the Council, The European Economic and Social Committee and the Committee of the Regions, Digitising European Industry Reaping the Full Benefits of a Digital Single Market SWD/2016/0110 final, Available: http:// eur-lex.europa. eu/legal-content/ EN/TXT/?uri= CELEX:52016SC0110 [Accessed: 11 March 2017].

122. Thornberry, C. (2017) Internet of things-enabled servitization for small to medium sized enterprises: innovation report, Doctoral dissertation, University of Warwick.

123. Tukker, A., and Tischner, U. (2006) Product-services as a research field: past, present and future, Reflections from a decade of research, Journal of cleaner production, 14(17), pp. 1552-1556.

124. Turber, S., Vom Brocke, J., Gassmann, O., and Fleisch, E. (2014) Designing business models in the era of internet of things, In International Conference on Design Science Research in Information Systems, pp. 17-31, Springer, Cham.

125. Upadhyay, J.S. (2017) Complexity - A Major IoT Challenge, [Online], Available: https:// community.hitachivantara. com/community/ iot/blog/2017/ 09/07/complexity- a-major-iot- challenge [Accessed: 12 May 2018].

126. Wadhwa, P., and Puri, A. (2016) Internet of Things: Challenges and impact, International Journal of Engineering Research and General Science Volume 4, Issue 3, May-June, 2016.

127. Van Alstyne, M. W., Parker, G. G., and Choudary, S. P. (2016) Pipelines, platforms, and the new rules of strategy, Harvard Business Review, 94(4), 54-62.

128. Van Der Wees, A., Breeuwsma, J. and Van Sleen, A. (2016) IoT Societal Impact - Legal Considerations and Perspectives, Digitizing the Industry - Internet of Things Connecting the Physical, Digital and Virtual, River publishers series in communication, Vol 49, pp. 215-235.

129. Vandermerwe, S., and Rada, J. (1988) Servitization of business: adding value by adding services, European management journal, 6(4), pp. 314-324.

130. Vargo, S. L., and Lusch, R. F. (2004b), The four service marketing myths: remnants of a goods-based, manufacturing model, Journal of service research, 6(4), pp. 324-335.

131. Vargo, S. L., and Lusch, R. F. (2004a) Evolving to a new dominant logic for marketing, Journal of marketing, 68(1), pp. 1-17.

132. Wasserman, S. (2016) Top 5 Challenges to Implementing an IIoT System, [Online], Available: https:// www. engineering. com/ IOT/ ArticleID/ 12882/ Top-5- Challenges- to-Implementing- an-IIoT-System. aspx [Accessed: 11 May 2018].

133. Weber, R.H. (2013) Internet of things - governance quo vadis?, Computer Law & Security Review 29.4 (2013), pp.341-347.

134. Westerlund, M., Leminen, S., and Rajahonka, M. (2014) Designing business models for the internet of things, Technology Innovation Management Review, 4(7), 5.

135. Wheatley, M. (2013) Internet of Things vs. The Industrial Internet: What's the Difference?, [Online], Available: https:// siliconangle. com/blog/ 2013/06/ 04/internet- of-things- vs-the- industrial-internet-whats-the- difference/ [Accessed: 27 July, 2018].

136. Wu, M., Lu, T. J., Ling, F. Y., Sun, J., and Du, H. Y. (2010), Research on the architecture of Internet of things, In Advanced Computer Theory and Engineering (ICACTE), 2010 3rd International Conference, Vol. 5, pp. V5-484, IEEE.

137. Yan, Z., Zhang, P. and Vasilakos, A.V. (2014) A survey on trust management for Internet of Things, Journal of network and computer applications, 42 (2014), pp. 120-134.

138. Yin, R.K. (1981) The case study as a serious research strategy. Knowledge, 3(1), 97-114.

139. Ziegeldorf, J.H., Morchon, O.G. and Wehrle, K. (2014) Privacy in the Internet of Things: threats and challenges, Security and Communication Networks 7.12 (2014), pp.2728-2742.